




Department of Defense Intelligence Information System (DoDIIS)

Instructions 2000

February 2000



Prepared by:
DoDIIS Management Board

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 01022000	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Department of Defense Intelligence Information System (DoDIIS) Instructions 2000		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) DoDIIS Management Board		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms "IATAC COLLECTION"		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 118		

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 02/04/00	3. REPORT TYPE AND DATES COVERED Report	
4. TITLE AND SUBTITLE Department of Defense Intelligence Information System (DoDIIS) Instructions 2000 February 2000			5. FUNDING NUMBERS	
6. AUTHOR(S) Dennis G. Clemm				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church, VA 22042			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-AI 8725 John J. Kingman Road, Suite 944			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This report implements DoD 5000- and 4630-Series acquisition and interoperability directives for the Defense Intelligence Community. The DoDIIS Instructions 2000: (1) Provides technical guidance for developing, testing, fielding, and sustaining all infrastructure and mission applications that are to be integrated at DoDIIS sites; (2) Provides fiscal guidance for developing and submitting Service and Agency program submissions.				
14. SUBJECT TERMS INFRA			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT Unlimited	

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Approval of the *DoDIIS Instructions 2000*

1. *Department of Defense Intelligence Information System (DoDIIS) Instructions*

2000 (enclosed) implements DoD 5000- and 4630-Series acquisition and interoperability directives for the Defense Intelligence Community. The *DoDIIS Instructions 2000*:

- Provides technical guidance for developing, testing, fielding, and sustaining all infrastructure and mission applications that are to be integrated at DoDIIS sites.
- Provides fiscal guidance for developing and submitting Service and Agency program submissions.

2. *DoDIIS Instructions 2000* applies to all organizations and project managers fielding intelligence information technology capabilities to DoDIIS sites or converging or interfacing with the DoDIIS infrastructure.

3. These Instructions reflect existing DoDIIS architectural concepts and constructs. The DoDIIS Management Board fully expects the DoDIIS architecture to change as the Intelligence Community responds to requirements to provide more timely, direct intelligence to the Warfighter. Programs such as the Joint Intelligence Virtual Architecture (JIVA) Enterprise, initiatives such as Intel for the Warfighter (IFTW), and community assessments such as the DoDIIS Test Process Study are producing new and innovative ways to view and define the DoDIIS architecture. These newly defined features and capabilities are expected to promote increased interoperability between the DoDIIS and Global Command and Control System (GCCS) communities. This year, we begin the process of evolving the DoDIIS Instructions to address the JIVA Enterprise Architecture with Internet technologies and commercial applications. To maintain currency with these evolving concepts and capabilities, these Instructions will be updated annually.

4. The DoDIIS System Integration Management Office (SIMO) will manage the process to maintain these Instructions, ensuring that they continue to accurately reflect DMB direction.

FOR THE DIRECTOR:

//SIGNED//

1 Enclosure

DENNIS G. CLEM
Defense Intelligence Functional
Manager for Infrastructure

EXECUTIVE SUMMARY

These Instructions:

- Implement the Department of Defense 5000- and 4630-series acquisition and interoperability Directives and are consistent with the Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act of 1996); *Defense Information Infrastructure Master Plan*; and the *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Framework*.
- Provide management and technical guidance to support the DoD Intelligence Information System (DoDIIS) Community goal of attaining the intelligence mission capabilities envisioned in Joint Vision 2010.
- Reflect the continuing effort to build and implement a common framework for interoperability across the Intelligence and Defense Communities.
- Provide guidance and direction to organizations developing, testing, fielding, and sustaining Intelligence Mission Applications (IMAs) for the DoDIIS Community.
- Provide guidance and direction to DoDIIS management and sites in the areas of Defense Information Infrastructure compliance, testing and evaluation, distribution, training, information technology security, and the programming and budgeting processes.
- Provide guidance and direction to build a common, standardized set of policies, guidance, processes, and procedures for the acquisition and fielding of information technology capabilities that satisfy intelligence mission requirements for the DoD.

These Instructions are designed to improve interoperability and save critical resources across the Intelligence Community. The *DoDIIS Instructions 2000* will be updated annually to remain current and provide renewed direction.

Key changes in this document (from the April 1999 Instructions) include:

- For acquisition management, the DoDIIS Management Board (DMB) business process was streamlined, thus expediting voting and returning vote results to project managers (PMs); a comprehensive PM life cycle management checklist was developed; the Defense Intelligence Functional Manager for Infrastructure is designated as Milestone Decision Authority for Defense Intelligence Agency (DIA) systems; and all existing DoDIIS acquisition management guidance has been merged into this document.
- With respect to technical direction, developers must plan to support the Warfighter Common Operational Picture and strive to achieve DII COE level compliance; the Director of Central Intelligence's Mobile Code Policy has been adopted; and the responsibility for developing common system configurations is delegated to all members of the community.
- For messaging services, compliance with *AUTODIN Bypass System Global Routing Plan*, *System Operating Instructions*, and *Security Implementation Plan* is required; compliance with *DoDIIS Community Defense Message System (DMS) Design Architecture* is required; messaging development and implementation actions are delegated to the DoDIIS DMS Sites Working Group; and leveraging resources where messaging infrastructures converge is mandated.

- For dissemination, specific guidance is issued to PMs, the DoDIIS Test Facility, DoDIIS management staff, and DoDIIS sites.
- For training, the Instructions more clearly state the intent to transition from formal classroom training to embedded, distance, and collaborative training.

Throughout these Instructions effective dates for assigned tasks have been removed. Instead a DoDIIS Calendar will be developed and maintained separately. The DoDIIS Calendar will identify dates for completing mandated taskings, with relative dates assigned to tasks in which DoDIIS is dependent upon the actions of an external organization. All dates appearing in the DoDIIS Calendar will be approved by either the DoDIIS Management Board or the DoDIIS Review Board (DRB). The DoDIIS Calendar will be updated and maintained by the DoDIIS Secretariat, accessed via the DMB Home Page on Intelink, and reviewed at each DRB and DMB meeting.

.

CONTENTS

Approval Memorandum.....	2
Executive Summary	3
Table of Contents	5
List of Figures.....	9
List of Tables	9
Section 1 – Introduction	11
1.1 Purpose.....	11
1.2 Background	11
1.3 Applicability.....	13
1.4 Key DoDIIS Activities.....	13
1.5 Document Organization.....	15
1.6 Effectivity.....	15
1.7 Compliance Constraints	15
1.8 Impact Assessment.....	15
1.9 Supersession.....	15
Section 2 – DoDIIS Acquisition Management	17
2.1 Overview	17
2.2 Integration Management Principals	17
2.2.1 Director, DIA	17
2.2.2 Milestone Decision Authority.....	17
2.2.3 DoDIIS Management and Review Boards.....	18
2.2.4 DMB Member Organizations.....	19
2.2.5 DoDIIS SIMO	19
2.2.6 DoDIIS Engineering Review Board	20
2.2.7 DoDIIS Executive Agent (DExA) for Test and Evaluation	20
2.2.8 DoDIIS Distribution Facility Responsibilities.....	20
2.2.9 Project Manager	20
2.3 DoD Acquisition Management Milestones and Phases	21
2.3.1 Milestone 0.....	21
2.3.2 Phase 0---Concept Exploration.....	22
2.3.3 Milestone I---Approval to Begin a New Acquisition.....	22
2.3.4 Phase I---Program Definition and Risk Reduction	22
2.3.5 Milestone II --- Approval to Develop	22
2.3.6 Phase II --- Development.....	23
2.3.7 Milestone III --- Fielding/Deployment Approval	23
2.3.8 Phase III --- Fielding and Operational Support.....	23
2.3.9 Waivers	24
2.4 DMB Acquisition Decision Memorandum Review Process	24
Section 3 – DII Compliance Guidance	27
3.1 Overview.....	27
3.1.1 Implementation of a DII COE Infrastructure	27

3.1.2	DII COE Compliance.....	28
3.1.3	DoDIIS Support to the COP.....	29
3.1.4	Effectivity Dates and DoDIIS Segments.....	29
3.1.5	DoDIIS Configuration Definitions.....	29
3.2	Fielding New DII COE and IMA Releases.....	30
3.3	Application Development and Segmentation.....	30
3.3.1	Segmentation of DoDIIS IMAs	30
3.3.2	Segment Registration.....	31
3.4	DII COE I&RTS Compliance Goals.....	32
3.4.1	General Segmentation Considerations	32
3.4.2	Functional Decomposition.....	32
3.4.3	Data Standardization/Segmentation.....	33
3.5	General Technical Guidance	34
3.5.1	Standards.....	34
3.5.2	Operating Systems	34
3.5.3	Support for Web and Multi-tiered Architectures	35
3.5.4	Object-Computing Technologies	35
3.5.5	Mobile Code.....	35
3.5.6	Reuse.....	36
3.5.7	Support for Low Bandwidth Communications	36
3.5.8	Consolidated Application Server Requirements	36
Section 4 – DoDIIS Testing and Evaluation.....		39
4.1	Overview.....	39
4.2	DoDIIS Testing and Evaluation Policy.....	40
4.3	Year 2000 Compliance.....	42
4.4	User Participation.....	42
Section 5 – DoDIIS Distribution.....		45
5.1	Overview.....	45
5.2	DoDIIS Asset Repository.....	45
Section 6 – Training		47
6.1	Overview.....	47
6.2	Approach to Satisfying DoDIIS Training Requirements	47
6.2.1	Institutional Training.....	48
6.2.2	Technology-Based Training.....	48
6.3	Training Management Plan.....	49
6.4	Training Certification.....	49
Section 7 – Information Systems Security		51
7.1	Overview	51
7.2	DoDIIS Security Certification Process	51

Section 8 – Budget Approval Process.....	55
8.1 Overview.....	55
8.2 GDIP Budget Approval Process	55
8.3 Project Manager GDIP Resource Responsibilities	56
8.4 Service/Command/Agency SIMO Responsibilities.....	58
8.5 DoDIIS SIMO Responsibilities	58
8.6 Resource/Functional Managers Responsibilities	58
8.7 Site Transition Planning Responsibilities	58
Section 9 – DoDIIS Messaging	61
9.1 Overview.....	61
9.2 Transitional Messaging (i.e., AUTODIN Bypass).....	61
9.3 Full DMS Implementation	61
Appendix A – List of Taskings.....	63
A.1 Section 1-Introduction.....	63
A.2 Section 2-DoDIIS Acquisition Management.....	63
A.3 Section 3-DII Compliance Guidance	67
A.4 Section 4-DoDIIS Testing and Evaluation.....	68
A.5 Section 5-DoDIIS Distribution	70
A.6 Section 6-Training.....	70
A.7 Section 7-Information System Security	71
A.8 Section 8-GDIP Budget Approval Process	72
A.9 Section 9-DoDIIS Messaging	73
Appendix B - Supplemental Technical Information.....	75
B.1 Description of DII COE.....	75
B.1.1 DII COE Layered Architecture	75
B.1.2 Building a DII COE-Based Infrastructure.....	75
B.1.3 DII COE Levels of Compliance.....	77
B.2 Description of the Common Operational Picture (COP)	77
B.3 DoD Joint Technical Architecture	79
Appendix C – DoDIIS Acquisition.....	81
C.1 Required Documents for Each Milestone	81
C.1.1 Preparation for Milestone 0.....	81
C.1.2 Preparation for Milestone I	82
C.1.3 Preparation for Milestone II.....	83
C.1.4 Preparation for Milestone III.....	84
C.2 Acquisition Program Baseline Format.....	85
C.3 ADM Format and Content	88
Appendix D – DMB Mobile Code Policy.....	99
Appendix E – DII COE Product Sponsorship.....	101

Appendix F – Public Key Infrastructure	103
Appendix G – References.....	107
Appendix H – Glossary of Acronyms	115

List of Figures

Figure 1.1 – DMB Member Organizations	12
Figure 1.2 – DoDIIS Enterprise	12
Figure 2.1 – Principal Offices and Organizations Involved in the Acquisition Process.....	18
Figure 2.2 – Milestone Decision Points and Phases	21
Figure 4.1 – Testing and Certification Process	41
Figure 4.2 – Testing and Certification Milestones.....	43
Figure 6.1 – Training Management Plan.....	50
Figure 8.1 – GDIP Build Process.....	56
Figure B-1 – DII COE Architecture	76
Figure B-2 – Notional DoDIIS Configuration.....	76
Figure B-3 - DII COE Levels of Compliance.....	78
Figure C-1 – Acquisition Program Baseline Format	88
Figure C-2 – Acquisition Decision Memorandum for Milestones I-II.....	89
Figure C-3 – Acquisition Decision Memorandum for Milestone III.....	90
Figure C-4 – Program Manager’s Checklist	97

List of Tables

Table 1.1 – Key DoDIIS Activities.....	14
Table 1.2 – Key Recurring DoDIIS Milestones.....	14
Table 7-1 – Sample SRTM Format.....	53
Table C-1 – DoDIIS Documentation Requirements.....	81

SECTION 1

INTRODUCTION

1.1 PURPOSE

The Department of Defense Intelligence Information System (DoDIIS) process transforms functional and technical requirements into mission capabilities. The process implements the Department of Defense (DoD) 5000- and 4630-series acquisition and interoperability directives and is consistent with the Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act of 1996 (ITMRA)); *Defense Information Infrastructure (DII) Master Plan*; and *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework*. This document provides management and technical guidance to support the DoDIIS Community goal of attaining the intelligence mission capabilities envisioned in Joint Vision 2010 (JV 2010), and reflects the continuing effort to build and implement a common framework for interoperability across mission areas.

The policy prescribes the enterprise-wide management processes and procedures that will be used to ensure the delivery of interoperable, functionally robust applications that satisfy warfighter operational requirements. *DoDIIS Instructions 2000* provides the technical guidance for developing, testing, fielding, and sustaining all infrastructure and mission applications that are to be integrated at DoDIIS sites.

These Instructions provide guidance and direction to build a common, standardized set of policies, guidance, processes, and procedures for the acquisition and fielding of information technology capabilities that satisfy intelligence mission requirements for the DoD. The goal is to improve interoperability and save critical Intelligence Community (IC) resources.

1.2 BACKGROUND

The *DoDIIS Instructions 2000* reflect the evolving nature of the DoDIIS Community and its relationships and interdependencies with other DoD and Intelligence Community entities. Figure 1-1 depicts the current configuration of the DoDIIS Management Board (DMB) and its relationship to the Military Intelligence Board (MIB). The Director, Defense Intelligence Agency (DR/DIA) serves as the Director of Military Intelligence (DMI) and Chairs the MIB. The DMB is chaired by the Defense Intelligence Functional Manager for Infrastructure (DIFM-I).

Figure 1-2 reflects an enterprise perspective and the interrelationships within the DoDIIS Community needed to manage, develop, test, train, field, and sustain an infrastructure and the intelligence mission applications needed to satisfy mission requirements. The term “intelligence mission application” or “IMA” is used in these Instructions to emphasize the need to use a community-centric vice systems-centric approach when delivering software capabilities to the field. The community-centric approach to acquiring information technology (IT) capabilities permits individual DoDIIS sites to acquire, integrate, install, and maintain an infrastructure that

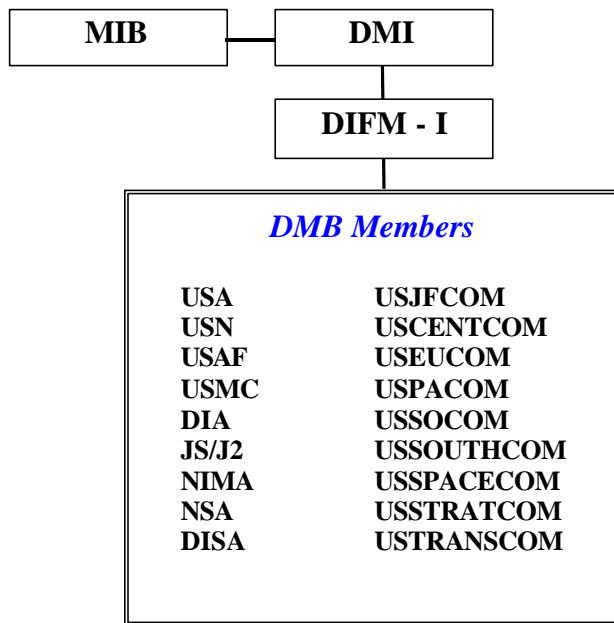


Figure 1-1 DMB Member Organizations

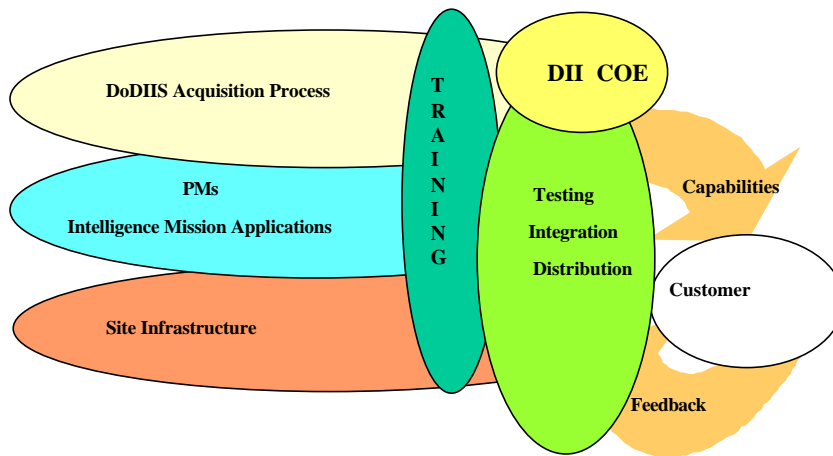


Figure 1-2. DoDIIS Enterprise

meets their specific mission requirements. The transition to a community-centric approach is also consistent with the DMB decision to implement an accreditable Defense Information Infrastructure Common Operating Environment (DII COE) throughout the DoDIIS Community, using an enterprise approach to achieving the highest levels of compliance.

Because members of the IC have historically used different terminology to represent similar concepts and constructs, these Instructions use the term “intelligence mission application” and “IMA” as a replacement for migration systems, mission specific application, analytic tool, and cognitive tool. In this context, an IMA may be either a commercial off-the-shelf (COTS) or government developed application.

From an enterprise perspective, the transition to DII COE requires considerable attention to compliance verification and configuration management (CM) at both the project and enterprise levels. To achieve this continuum of CM required expanding the functions of and cooperation among the project managers (PMs), Joint Integration Test Facility (JITF), Joint Interoperability Test Command (JITC), and Joint Deployable Intelligence Support System Joint Program Office (JDISS JPO). These increased responsibilities and greater cooperation ensure that acquired IT capabilities meet requirements and specifications, and that only DMB approved software that is certified by a Milestone Decision Authority (MDA) is brought under enterprise CM through the DoDIIS Asset Repository and made available to DoDIIS sites.

1.3 APPLICABILITY

This document applies to the DMB member organizations and the reserve intelligence organizations, as well as organizations that acquire or develop capabilities to be integrated into DoDIIS sites. Unless otherwise specified, these Instructions do not apply to site-unique applications that have no requirements to provide data or capabilities to analysts and applications external to the site.

Within the Instructions each tasking is uniquely identified with a number. A tasking with a "shall" indicates that there is an expectation of and commitment by the DMB member organizations to adopt and to support programmatically, contractually, and architecturally the intent of each "shall" statement. It also means that if an organization cannot comply for some reason, then that reason will be brought by that organization to the attention of the DMB.

A tasking with a "should" indicates that there is an expectation of and commitment by the DMB member organizations to work toward the desired end-state. Appendix A contains a consolidated list of all taskings.

INI These Instructions should be used as the basis for:

- Fiscal Years (FY) 2000 and 2001 implementation and as planning factors for the FY2002-2007 Intelligence Program Objective Memorandum (IPOM).
- Any contract awarded after approval of this document.

1.4 KEY DODIIS ACTIVITIES

Table 1-1 identifies some key DoDIIS activities that are discussed in subsequent sections of this document. Table 1-2 highlights key recurring milestones that affect DoDIIS.

Throughout these Instructions effective dates for completing assigned tasks have been removed. Instead a DoDIIS Calendar will be developed and maintained separately. The DoDIIS Calendar will identify dates for completing mandated taskings, with relative dates assigned to tasks in which DoDIIS is dependent upon the actions of an external organization. All dates appearing in the DoDIIS Calendar will be approved by either the DMB or the DoDIIS Review Board (DRB). The DoDIIS Calendar will be updated and maintained by the DoDIIS Secretariat, accessed via the DMB Home Page on Intelink, and reviewed at each DRB and DMB meeting.

Table 1-1. Key DoDIIS Activities

ACTIVITY	APPLIES TO
Develop Calendar/Schedule for Completing Key Activities	DMB, SIMO and ERB
Define Requirements for DoDIIS Migration to DII COE	DMB and DRB
Develop and Field an Accredited DII COE Infrastructure	PMs, Sites, DoDIIS Distribution Facility, JITF
Segment and Test IMAs	PMs and DoDIIS Test Agencies
Complete the transition to Solaris and NT OSs, except as noted in para 3.5.2	PMs, JITF, Sites
Terminate support for all applications and site environments not based upon DoDIIS Migration to DII COE and the Target Operating Systems (TOSs), except as noted in para 3.5.2	PMs, Sites
IMAs segmented and certified to field	PMs, Services, Sites, DoDIIS Test Agencies
Complete AUTODIN Bypass Implementation and AUTODIN shutdown	DoDIIS Community Sites
Transition to technology-based training delivery methods	PMs, Sites, Joint Regional Training Centers

Table 1-2. Key Recurring DoDIIS Milestones

RECURRING ACTIVITY	APPLIES TO	DATE
DoDIIS Instructions	DMB Member Organizations	1 October
Program Guidance (e.g., Defense Planning Guidance, Joint Intelligence Guidance, Program Manager's Guidance Memorandum, Supplemental Cost Guidance)	DMB Member Organizations	1 October
APB updated, posted on Intelink and Intelink-S	PMs and DExAs/PEOs	At each milestone and 1 November
IPOM Reviews	DS-IM	April-May
Site Transition Plans (STP) updated	Sites SIMOs	1 December
Test/integrate/disseminate new DII COE releases	DoDIIS Community	Biannual

1.5 DOCUMENT ORGANIZATION

DoDIIS Instructions 2000 is organized into nine major sections and eight appendices. Instructions for DoDIIS Executive Agents (DExAs), Program Executive Officers (PEOs), PMs, and DoDIIS sites that are acquiring and developing IT capabilities are included throughout the document.

Section 2 focuses on the DoDIIS Acquisition Management process and provides an overview of the roles and responsibilities of the principal organizations involved in implementing the process. Section 3 contains general and technical guidance concerning transition to the DII COE and development of segmented IMAs. Section 4 elaborates on instructions for Testing and Evaluation of DoDIIS IMAs. It reflects an evolving role for the Joint Integration Test Facility (JITF) as the DoDIIS Test Facility with responsibility for ensuring IMA compliance with *DoDIIS Instructions 2000*. Section 5 expands the JDISS JPO role to be the DoDIIS Distribution Facility and manager of the DoDIIS Asset Repository, facilitating the distribution of the DII COE and segmented IMAs. Section 6 reflects increased emphasis on new training delivery methods to increase the effectiveness of training while decreasing the total cost over IMA life cycle. Section 7 reflects current security guidance and direction, and Section 8 reflects the General Defense Intelligence Program (GDIP) and IPOM review process. Section 9 presents actions required to implement both transitional messaging and the Defense Message System (DMS) in full.

Each Uniform Resource Locator (URL) identified in this document is an Internet address, unless otherwise specified.

1.6 EFFECTIVITY

These Instructions are effective upon signature.

1.7 COMPLIANCE CONSTRAINTS

IN2 When there is a conflict between these Instructions and another DoDIIS document, these Instructions shall have precedence. When there is a conflict between these Instructions and an approved DoD policy document, the DoD policy shall take precedence (e.g. DoD 5000 directive). Exceptions to this policy can be granted by the DMB.

1.8 IMPACT ASSESSMENT

IN3 If any instruction in this document cannot be accomplished because of insufficient fiscal resources or has negative performance, schedule, or risk impact, the affected organization shall brief the DMB and detail the impact in their FY2002-2007 IPOM using the Format 9 or Format 7 (or equivalent for DoDIIS organizations that do not use these Formats).

1.9 SUPERSESSION

This document supersedes the *DoDIIS Instructions*, dated April 1999.

SECTION 2

DODIIS ACQUISITION MANAGEMENT

2.1 OVERVIEW

The DoDIIS acquisition management process implements DoD Directive 5000.1 and DoD 5000.2-R under the guidance of the Clinger-Cohen Act. IMAs are developed by a number of organizations such as the Defense Intelligence Agency (e.g., Modernized Integrated Database), a Service (e.g., Army for Joint Collection Management Tools), or another Defense Agency (e.g., Image Product Library developed by the National Imagery and Mapping Agency (NIMA)). For purposes of this section, a distinction is made between IMAs developed by the DIA and those developed by a Service or Defense Agency (referred to as Service/Agency) for fielding at a DoDIIS site. This distinction is made because of Title 10 and acquisition oversight responsibilities.

2.2 INTEGRATION MANAGEMENT PRINCIPALS

The offices and organizations that have primary responsibility for implementing the DoDIIS acquisition management process are shown in Figure 2-1.

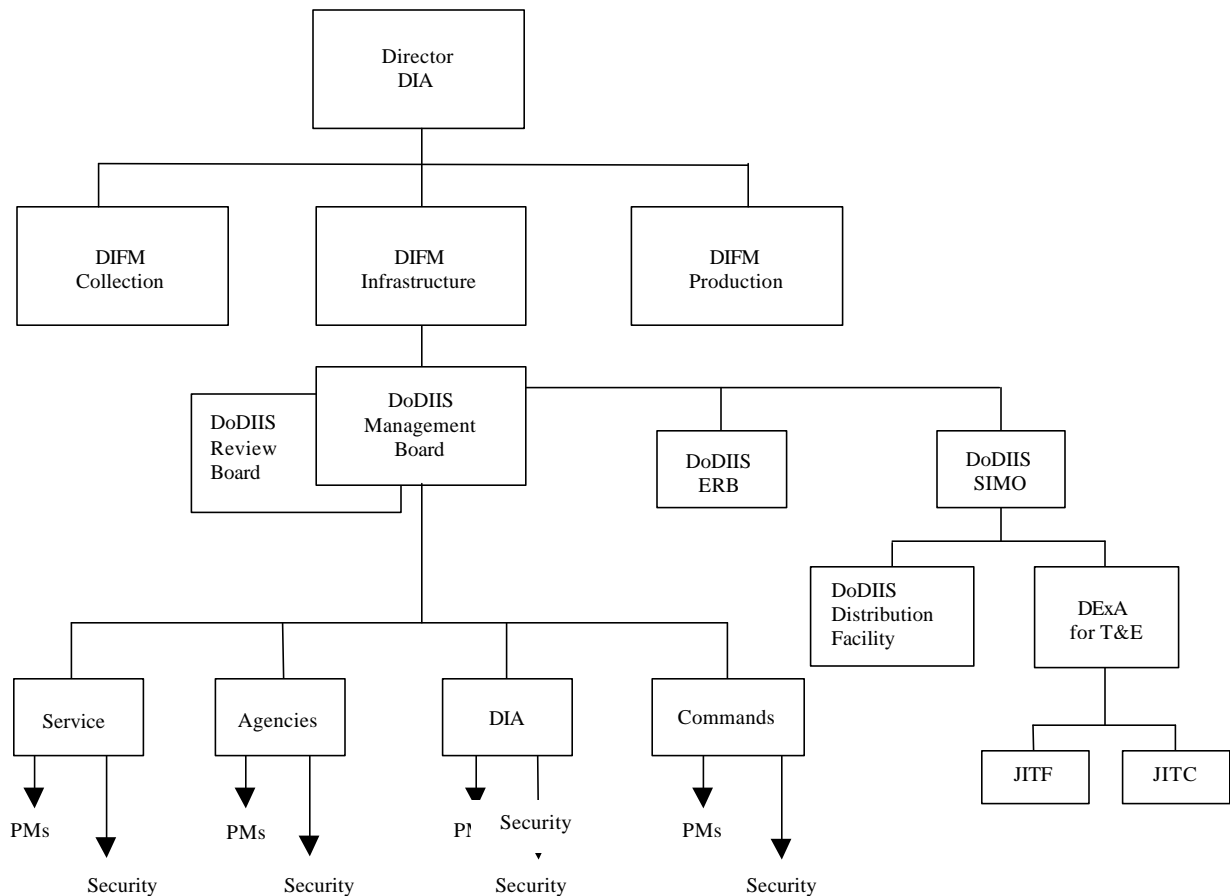


Figure 2-1. Principal Offices and Organizations Involved in the Acquisition Process

2.2.1 Director, DIA

The DR/DIA is responsible for oversight of the research and development, procurement, and operation of DoD intelligence infrastructure-related programs, systems, and activities funded in the GDIP. The DR/DIA:

- Implemented the DoDIIS acquisition management and approval process in accordance with DoD Directive 5000.1 and DoD 5000.2-R, consistent with Information Technology and acquisition statutes, regulations, and other Office of Secretary of Defense (OSD) guidance.
- Designated the DMB as the senior joint review board for the DoDIIS acquisition management process.
- Designated the DIFM-I as MDA to review, coordinate on Acquisition Decision Memoranda (ADMs), and issue a Certificate to Field for major and minor IMA releases.

2.2.2 Milestone Decision Authority

The MDA for DIA-developed IMAs is the DIFM-I. The Component Acquisition Executive within other DoD Components (i.e., Service, Defense Agency, and Command) designates the MDA for the Service/Agency IMAs in accordance with (IAW) Title 10 and the DoD 5000-series acquisition directives.

AC1 The DIFM-I shall:

- Implement and oversee the DoDIIS acquisition management process, to include Clinger-Cohen Act specified acquisition and system management processes.
- Review requirements at each milestone in accordance with OSD direction.

2.2.3 DoDIIS Management and Review Boards

The DMB is a decision making body chartered by the Military Intelligence Board (MIB). The MIB is chaired by DR/DIA; the DMB is chaired by the Defense Intelligence Functional Manager for Infrastructure (DIFM-I). The DoDIIS Review Board (DRB), which is chartered by the DMB, supports the DMB in its decision-making role by conducting technical and functional reviews and analyses, providing a forum for the user community, and ensuring milestone readiness for information technology capabilities being fielded at DoDIIS sites. Together, the DMB and DRB, assisted by the DoDIIS Management Division, provide integrated recommendations and assessments to the cognizant MDA at each acquisition milestone decision point. (A description of the DMB business process is accessible from the DoDIIS Intelink Home Page – <http://www.dia.ic.gov/proj/dodiis/dodiis.html>.)

AC2 The DMB Chair shall:

- Issue a Certificate to Field for all major and minor releases (as defined in Section 3.2) of DIA IMAs, based on recommendations from the DRB/DMB.
- Coordinate on Certificates to Field for all major and minor releases of Service and Agency IMAs being fielded at more than one DoDIIS site, based on recommendations from the DRB/DMB.

AC3 The DMB shall:

- Serve as the senior joint review board for all DoDIIS acquisition management actions.
- Provide recommendations to the DMB Chair and the appropriate Service/Agency MDA concerning milestone achievement and the issuing of a Certificate to Field.
- Approve the inclusion of new software applications or tools into the DoDIIS Asset Repository, maintained by and accessible through the DoDIIS Distribution Facility (see Section 5 for added discussion of the DoDIIS Distribution Facility).
- Approve IMA software releases to be placed in the DoDIIS Asset Repository.

AC4 The DRB Chair shall review and approve or reject the recommendation from the DoDIIS Test Facility concerning maintenance releases (as defined in Section 3.2), and, if approved, issue a Certificate to Field (see Section 4 for added discussion of the DoDIIS Test Facility).

2.2.4 DMB Member Organizations

DMB member organizations must implement the DoDIIS acquisition management process within their area of responsibility, to include Clinger-Cohen Act specified acquisition and system management processes. These responsibilities include reviewing requirements at each milestone with the cognizant MDAs.

2.2.5 DoDIIS SIMO

The DoDIIS SIMO provides staff support to the DMB and facilitates PM, DExA, DMB, and MDA interaction. The DoDIIS SIMO interfaces with and supports the PMs to ensure an understanding of and adherence to milestone requirements. DoDIIS SIMO actions and activities promote an understanding of DoDIIS integration and interoperability objectives by facilitating interaction among IMA PMs.

AC5 The DoDIIS SIMO shall:

- Provide recommendations to the DMB and DRB regarding milestone achievement and system readiness in support of Milestone I-III decisions.
- Coordinate with PMs to ensure adherence to DoDIIS Certification Process.
- Facilitate the day-to-day acquisition management process for the DoDIIS members.
- Review ADM packages for relevant Milestone information, coordinate with the appropriate organizations (e.g., DoDIIS Engineering Review Board (ERB), Security, and Training), and prepare recommendations for DMB/DRB consideration.
- Preview the recommendation from the DoDIIS Test Facility concerning maintenance releases prior to submission to the DRB Chair for approval.
- Notify the DoDIIS Test Facility that a Certificate to Field has been issued.

2.2.6 DoDIIS Engineering Review Board

The DoDIIS ERB provides engineering and technical staff support to the DMB. The ERB reviews the submitted ADM and attachments from an engineering and technical perspective. If needed, the

ERB attends meetings with the PM to mitigate deficiencies in the documentation or problems identified in reports. A written analysis from the ERB is delivered to the DoDIIS SIMO within five working days following receipt of the ADM.

2.2.7 DoDIIS Executive Agent (DExA) for Test and Evaluation

The responsibilities of the DExA for Test and Evaluation include developing test policy in coordination with members of the Test Process Oversight Committee (TPOC); providing oversight of the test preparation, scheduling, testing, and reporting process; and serving as drafter of and primary advocate for the test process budget.

The Joint Integration Test Facility (JITF) and the Joint Interoperability Test Command (JITC) are the two primary organizations supporting the DExA for Test and Evaluation. The JITF is responsible for all integration, compliance, and installation testing and documentation review. The JITC is responsible for all interoperability testing. See Section 4 for more detailed information on testing.

2.2.8 DoDIIS Distribution Facility Responsibilities

The DoDIIS Distribution Facility (DDF) will be the single point of distribution for DoDIIS certified software. See Section 5 for more detailed information.

2.2.9 Project Manager

PMs are responsible for the design, development, project level integration and testing, and delivery of mission application segments (as discussed in Section 3 and Appendix B) that satisfy specific criteria established for functionality, performance, security, and training. Therefore:

- AC6** All PMs shall manage their respective software development efforts consistent with legislative, statutory and DoDIIS acquisition guidance. These Instructions include the format for preparation of an Acquisition Decision Memorandum and maintenance of a current Acquisition Program Baseline (APB) to ensure consistency with DoD 5000-series acquisition guidance (see Appendix C for the required ADM and APB format and content).
- AC7** All PMs shall validate, develop, certify and field their respective IMAs through the DoDIIS acquisition management process. This includes major, minor and maintenance releases.
- AC8** Service/Agency PMs shall coordinate their ADM for Milestones II and III with the DIA and DMB.
- AC9** DIA PMs shall have an ADM and a current, approved Acquisition Program Baseline (APB).
- AC10** All PMs shall coordinate their testing schedule through the DexA for Test and Evaluation the JITF, JITC and the appropriate Security test agency.
- AC11** All PMs shall coordinate their proposed Beta II testing site(s) with the DoDIIS SIMO and the approved DoDIIS site(s).

2.3 DODIIS ACQUISITION MANAGEMENT MILESTONES AND PHASES

The DoDIIS acquisition management process reflects the milestone decision points as defined in DoD 5000.2-R. Refer to DoD 5000.2-R for detailed information concerning acquisition phases and milestones, and documentation. Figure 2-2 shows the normal progression of these milestones and phases.

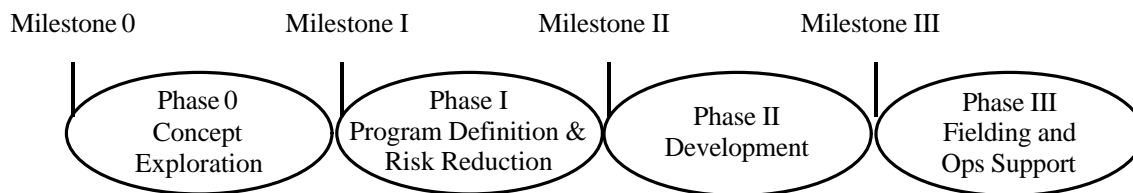


Figure 2-2. Milestone Decision Points and Phases

Phases and Milestones II and III may be repeated as necessary based on the acquisition and development process (i.e., incremental, evolutionary, spiral, or prototyping) for each DoDIIS IMA. The MDA may modify the number of phases, milestone decision points, and system documentation required to meet the specific needs and development of individual projects. At each milestone decision, the APB, which documents cost, schedule, and performance for the next phase, must be updated by the PM and revalidated by the MDA. The DoDIIS SIMO will work and interface with the Commands, Services, and Agencies to facilitate coordination among all organizations involved in the milestone decision process.

The types of documentation to be developed during each phase prior to each milestone review may be found in Appendix C. The MDA may provide waivers, as appropriate and recommended by the DMB and the DoDIIS SIMO.

2.3.1 Milestone 0

The Mission Needs Statement (MNS) approval by the cognizant acquisition executive is the Milestone 0 decision and the start of Phase 0 (Concept Exploration). DoDIIS components are reminded the Clinger-Cohen Act requires each Service/Command/Agency head to determine, before making an investment in a new information system: a) whether the function to be supported by the system should be performed by the private sector and b) whether the function should be performed by the Service/Command/Agency and if so, whether by contract or government personnel.

2.3.2 Phase 0 — Concept Exploration

During this phase the Operational Requirements Document (ORD) is approved by the cognizant acquisition executive and most of the initial program level documentation is begun (see Appendix C for a list of the required documentation). Activities in support of the Milestone 0 decision involve the refinement of validated requirements, the appointment of the MDA, and concept exploration. At this point the Defense Intelligence Functional Managers become involved. They determine whether the proposed functions are essential or duplicates of existing capabilities and provide this

information to the DMB. The DMB considers the proposed functions for inclusion in the DoDIIS Asset Repository. Those functions accepted into the inventory are to be developed according to the acquisition management process discussed in Sections 2.3.3 through 2.3.9.

2.3.3 Milestone I — Approval To Begin A New Acquisition

The Milestone I decision determines whether the results of Phase 0 warrant establishing a new, fully GDIP-funded IMA and to approve entry into Phase I. Concept exploration considers the existing capabilities and defines the unique requirements of the proposed application. The MDA, or designee, issues a decision memorandum, to include exit criteria for the next phase, and approves the APB.

2.3.4 Phase I — Program Definition and Risk Reduction

During Phase I, the PM specifies and documents the design and development procedures. The design specifications address issues related to: a) Joint Technical Architecture compliance; b) consistency with DoD data standards and initiatives; and c) identification of the functional capabilities to be satisfied in each incremental delivery. If prototyping is used during Phase I, the project office will document the evaluation and test results from the prototyping activities.

The PM will identify interfaces in Phase I and document the interface characteristics in an interface specification. During Phase I, the PM begins to develop initial test plans, security documentation, and training management plans; the PM will finalize these documents in Phase II. Test plans and procedures will be reviewed and validated by DoDIIS Test Facility personnel to ensure consistency with the testing and certification process.

2.3.5 Milestone II — Approval to Develop

A Milestone II decision determines whether the results of Phase I warrant continuing the program and approves entry into Phase II (Development). Based on a recommendation from the DMB, assisted by the DoDIIS SIMO, the MDA will approve/disapprove the ADM. For Service/Agency-developed IMAs entering the DoDIIS Asset Repository, the proposed functionality is reviewed by the DoDIIS Test Facility (with support from the ERB) for possible duplication with other applications residing in the DoDIIS Asset Repository. The DoDIIS Test Facility will provide a report to the PM, the DexA for Test and Evaluation, and the DoDIIS SIMO. This information will assist with the planning and implementation of the functional decomposition process discussed in Section 3.4.2.

2.3.6 Phase II — Development

During Phase II, the PM develops the requisite design and development documentation, as well as support documentation (such as version description documents and user manuals) and site configuration and installation guides. The objective is to ensure that IMAs can be fielded and maintained by individuals other than the developer. The amount of documentation will be consistent with the scope and size of the development and sound business practices. A list of the minimum documentation to be prepared is given in Appendix C.

DoDIIS IMAs may be developed and fielded using an incremental, evolutionary, or spiral approach. Each incremental delivery will be managed as a separate product. The first increment of all IMA deliveries will include all features needed to ensure DoDIIS architectural compliance. The priority of the requirements and the degree of risk associated with the product will determine the sequencing of the incremental products.

Interoperability across DoDIIS organizations and mission areas is critical. A key to ensuring that DoDIIS IMAs can interface electronically and exchange data prior to being fielded is interoperability testing.

All DoDIIS IMAs must also complete infrastructure compliance, integration, installation and security testing prior to receiving approval to field at one or more DoDIIS sites for Beta II testing. The DMB, assisted by the DoDIIS SIMO and DRB, makes recommendations to the MDA on approving deployment for Beta II tests. Before deploying to a Beta II test site, the PM must provide an ADM to the DoDIIS SIMO for interim Milestone III approval. PMs will coordinate their proposed Beta II testing site(s) with the DoDIIS SIMO and the approved DoDIIS site(s).

2.3.7 Milestone III — Fielding/Deployment Approval

A Milestone III decision, following Beta II Testing, authorizes the distribution of an IMA for integration and use by operational sites. For IMAs to obtain approval to field and receive a Certificate to Field, the PM submits an ADM to the DoDIIS SIMO following successful Beta II testing. The DoDIIS SIMO, in coordination with the DRB, DoDIIS Test Facility, JITC, and the ERB, will make recommendations to the DMB. Upon review, the DMB makes recommendations to the cognizant MDA regarding milestone decisions and whether to issue a Certificate to Field. A favorable recommendation can result in the DMB Chair issuing a Certificate to Field at DoDIIS sites for DIA IMAs, and will result in issuing of the Certificate to Field at DoDIIS sites for Service/Agency IMAs once their cognizant MDA has approved fielding. No IMA will be released for fielding at a DoDIIS site without a Certificate to Field.

2.3.8 Phase III — Fielding And Operational Support

During Phase III the PM is responsible for maintenance releases of the IMA. Maintenance releases are delivered to the DoDIIS Test Facility for review. If needed, the release is subjected to testing before notification is sent to the DoDIIS SIMO that a maintenance release is ready for inclusion in the DoDIIS Repository. The DoDIIS SIMO recommends the release to the DRB Chair without the milestone approval process. The DRB Chair determines if the maintenance release is to be included

in the DoDIIS Repository. All approved maintenance releases of segmented IMAs will be distributed through the Distribution Facility.

2.3.9 Waivers

Waivers may be issued for individual steps of the DoDIIS Certification Process at the discretion of the DMB and MDA. PMs must submit requests for waivers with supporting justification to the DoDIIS SIMO. The DoDIIS SIMO in coordination with the DoDIIS Test Facility will provide a recommendation to the DMB members. The DoDIIS SIMO will coordinate the DMB findings with the PM.

2.4 DMB ACQUISITION DECISION MEMORANDUM REVIEW PROCESS

MDA approval for specified activities is obtained using the ADM. At each milestone, MDA decision/certification is documented by an ADM upon completion of one acquisition phase and the initiation of the next (see Figure 2-2). Phases and Milestones II and III may be repeated as necessary based on the acquisition and development process (i.e., incremental, evolutionary, spiral or prototyping) for each DoDIIS IMA. At each milestone decision the APB must be updated by the PM and revalidated by the cognizant MDA.

ACI2 The DoDIIS SIMO in coordination with the IMA PMs shall review status (schedule and version development) and tailor the phases, milestones, testing requirements (coordinated with JITF) and documentation content requirements for each IMA.

The route that an ADM follows through the acquisition management process is determined by several factors. The primary determinant is the IMA release.

ACI3 Major and minor IMA releases shall follow the full acquisition management process, resulting in a Certificate to Field.

ACI4 Maintenance releases shall be reviewed by the JITF and JITC, to determine the need for testing, and provide a 'go/no go' recommendation to the DoDIIS SIMO concerning readiness to field. PMs can appeal 'no go' recommendations to the DRB Chair.

Who the MDA is, is a secondary determinant.

ACI5 For DIA-developed IMAs, the ADM shall follow the complete acquisition management process, with a Certificate to Field issued upon successful completion of Milestone III.

ACI6 The DMB shall recommend to the cognizant MDA the appropriate action concerning issuing a Milestone III decision and a Service/Agency Certificate to Field.

For Service/Agency-developed IMAs, the ADM reflects the decision of the MDA who was appointed by the Component Acquisition Executive (CAE). However, prior to Service/Agency MDA finalization of Milestone II and III ADMs, they should be presented to the DMB for review. The DMB will coordinate, coordinate with comments, or non-concur on the Milestone II and III ADMs to the cognizant MDA. As part of the Milestone III review, the DMB will also issue

favorably viewed IMAs with a Certificate to Field at DoDIIS sites, to be activated once the cognizant MDA approves IMA fielding.

AC17 For Service/Agency-developed IMAs, PMs shall present the ADM to the DoDIIS SIMO for review at Milestones II and III.

AC18 DIA PMs shall (for all Milestone decisions):

- Submit the complete ADM and approved documentation to the DoDIIS SIMO at least four weeks prior to the desired date of review/vote completion. (Sensitive situations requiring immediate processing will be accomplished in a two-week period as deemed appropriate by the DoDIIS SIMO or DMB.)
- Brief the DMB/DRB as required.

AC19 The DoDIIS SIMO shall:

- Coordinate reviews with other organizations (to include the DRB, DIFMs, CIO, and DoD Components, as appropriate) allowing a two week period for review. (Sensitive situations requiring immediate processing will be accomplished in a one-week period as deemed appropriate by the DoDIIS SIMO or DMB.)
- Prepare a decision paper for DMB consideration. The decision paper will incorporate PM supplied data along with analysis from other sources and will cite issues that could not be resolved. Information gained in reviewing the ADM, specifically from the APB, will be used in updating the master schedule maintained by the DoDIIS SIMO. This will include dates for future Milestone decisions, tests, and version releases. The decision paper will also contain a DoDIIS SIMO recommendation regarding the ADM request.
- Execute a DMB vote, allowing a two-week review by the DMB members. (Sensitive situations requiring immediate processing will be accomplished in a one-week period as deemed appropriate by the DoDIIS SIMO or DMB.)
- Record and maintain a ballot reflecting each members vote.
- Prepare an appropriate message and letter for the Milestone and post the results of the vote on Intelink within five working days.
- Provide the DMB Milestone recommendation (or coordination for Service/Agency IMAs) to the MDA.

SECTION 3

DII COMPLIANCE GUIDANCE

3.1 OVERVIEW

Implementation of the DII COE is DoD policy and a requirement levied by the Department of Defense on each DoD functional community (see <http://spider.dii.osfi.disa.mil/dii/> for a description of DII COE). The directive that mandates implementation of the DII COE for all C4I systems is the *DoD Joint Technical Architecture (JTA)*. Version 1.0 was approved by the Under Secretary of Defense and Assistant Secretary of Defense (ASD)/C3I on 22 August 1996. Subsequent releases of the DoD JTA and follow-on memorandums, such as the 23 May 1997 ASD/C3I Memorandum, *Implementation of the Defense Information Infrastructure Common Operating Environment Compliance* and the 14 May 1999 ASD/C3I Memorandum, *Implementation and Evolution of the Defense Information Infrastructure (DII) Common Operating Environment (COE)*, have reiterated and refined DoD direction.

Many factors affect the DoDIIS transition to the DII, including Year 2000 (Y2K) considerations; budget constraints; site acquisition schedules; time needed to re-engineer support, infrastructure, and mission applications; security considerations; and the DII COE development schedule. The schedule for completing testing and fielding of a TOP SECRET/Sensitive Compartmented Information (TS/SCI)-certified DII COE infrastructure is contained in the DoDIIS Calendar. The DoDIIS near-term objective is to ensure that all site application and data servers, which are used by IMAs, are configured with an SCI accredited DII COE infrastructure. Sites have the option of configuring workstations with a DII COE accredited infrastructure, but are not required to do so. Site workstations and application and data servers used by IMAs must be configured with the target operating systems (TOSs [see Section 3.5.2]).

DISA, in its role as executive agent for DII, configures and delivers new versions of the COE. Minor and major releases to the DII COE baseline are planned for delivery every 6 and 36 months, respectively.

3.1.1 Implementation of a DII COE Infrastructure

The DII COE, as released by DISA, is not configured for use within the DoDIIS TS/SCI operating environment. Therefore, the DMB must approve the implementation of a TS/SCI-certified DII COE version within DoDIIS, taking into account ERB and Command, Service, and Agency (C/S/A) recommendations and considerations. Each version release of DII COE that is considered for use within DoDIIS will be assessed as to its security posture for use within a TS/SCI operating environment and configured appropriately. All DoDIIS security assessments will be conducted and coordinated with representatives of the DoDIIS ERB, the TS/SCI accreditors, the DoDIIS Test Facility, and DoDIIS C/S/A participants. DISA will also be invited to participate in DII COE security assessments.

DCI The DMB shall identify the version release of DII COE that is to be used as the infrastructure baseline for the DoDIIS Community.

- DC2** The DII COE version release shall undergo a security assessment to determine the current security posture of the as-released DII COE kernel with respect to use in the TS/SCI operating environment.
- DC3** As required from the results of the security assessment, the DII COE kernel configured for DoDIIS shall undergo Security Certification while at the DoDIIS Test Facility.

As determined through the Security Certification, the configuration of a TS/SCI-certified DII COE version (DII COE kernel configuration, plus any additional segments required for TS/SCI certification) will be identified to the DMB.

- DC4** The DMB shall approve the initial TS/SCI-certified DII COE software infrastructure baseline that is to be used at DoDIIS sites and issue a Certificate to Field.

Future version releases of the DII COE will be assessed for their value to DoDIIS and organizations that DoDIIS interfaces with. When the DMB identifies a version release as required by DoDIIS, that release will be reviewed and analyzed to determine its security posture. The approval process followed for fielding subsequent DII COE releases will parallel that which is discussed above for the initial release.

3.1.2 DII COE Compliance

To complete the transition to DII COE, the DMB has defined a community implementation process that relies on close coordination among all DoDIIS organizations. The DoDIIS ERB and DoDIIS SIMO will work with the Command, Service, and Agency SIMOs to facilitate and ensure coordination of site DII COE planning and implementation activities. Implementing the community process requires that the following be completed once there has been delivery of a TS/SCI certifiable DII COE baseline:

- DC5** By the date specified in the DoDIIS Calendar, every PM shall deliver IMA segments that are, at a minimum, DII COE level 5 compliant, as defined in the DII COE *Integration and Runtime Specification* (I&RTS).
- DC6** Every DoDIIS site shall complete the transition of its installed computing and processing base to the DII COE standards and protocols by the date specified in the DoDIIS Calendar.

General segmentation guidelines are as follows:

- DC7** PMs developing segmented IMAs shall complete the checklist contained in the DII COE I&RTS and provide it to the DMB and the DoDIIS Test Facility with each release of their application.
- DC8** PMs shall refer to the DoDIIS Asset Repository, maintained by the DoDIIS Distribution Facility, to avoid duplication of effort. The DoDIIS Asset Repository contains segments and configurations approved by the DMB for employment in DoDIIS.
- DC9** The DoDIIS Test Facility shall verify the level of compliance for each segmented IMA. (See the DII COE I&RTS for more information on segment verification.)
- DC10** PMs shall develop to DII COE compliant application and data servers.

DC11 PMs shall support workstation platforms that are DII COE compliant and workstation platforms that are not DII COE compliant.

3.1.3 DoDIIS Support to the COP

On 20 August 1999, the Expanded Defense Resource Board issued Intelligence Production Decision Memorandum (IPDM) I identified five DoDIIS IMAs that are required to support warfighter requirements for intelligence data. As appropriate, these DoDIIS IMAs will use the COP as their mechanism for displaying intelligence data on warfighter workstations (see Appendix B for an explanation of the COP). To support the COP:

DC12 By the date specified in the DoDIIS Calendar, the PMs for the IMAs identified in IPDM I shall satisfy warfighter requirements by making, as appropriate, intelligence information available to the COP.

DC13 PMs developing IMAs to support the COP shall support a COP interface.

3.1.4 Effectivity Dates and DoDIIS Segments

DoDIIS will adopt the concept of “effectivity dates” to denote when an assured capability will be “in the field and mission ready.” Effectivity dates will be set by “required operational readiness dates.” Required operational readiness dates may be determined by the Military Intelligence Board (MIB), Military Communications-Electronics Board (MCEB), a Service Intelligence Chief, a Unified Commander, or a Combat Support Agency Director, as well as the DII COE Configuration Review Control Board (CRCB) for the DII COE. Once the DoDIIS effectivity dates have been approved by the DMB, they will be included in the DoDIIS Calendar.

DC14 All contracts let in support of the DMB member organizations shall construct their project level priorities and deliverables taking effectivity dates into consideration.

3.1.5 DoDIIS Configuration Definitions

The DII COE I&RTS defines a configuration definition as a collection of segments that are grouped together for installation convenience. DoDIIS configuration definitions are both physical and logical entities. Logically they are a composite or compendium of segment descriptions as defined in the DII COE I&RTS. Physically, they occur at three locations:

- At the DoDIIS Test Facility where each segment and configuration definition will be subjected to a stringent review for compliance with the DII COE I&RTS.
- At the DoDIIS Distribution Facility where each configuration definition will be accessible according to the requirements of the operational users.
- At DoDIIS sites.

DC15 After Security Certification of a DMB approved TS/SCI release of the DII COE (see Section 3.1.1) has been completed at the DoDIIS Test Facility, the ERB shall lead a community effort to identify the DII COE segments that apply to DoDIIS and recommend configuration definitions (which include the DoDIIS Baseline and applicable IMAs) for DoDIIS.

DC16 The DoDIIS Test Facility shall integrate and test each DoDIIS configuration definition upon release of each new version of the DII COE. Configuration definitions will not be fielded until a “Certificate to Field” is issued.

3.2 FIELDING NEW DII COE AND IMA RELEASES

As discussed in Section 3.1.1, new releases of the DII COE will be assessed for their value to DoDIIS and organizations that DoDIIS interfaces with. When the DMB identifies a DII COE version release as required by DoDIIS, that release would be installed at DoDIIS sites only after it has been tested and approved for fielding.

DC17 All DoDIIS sites shall plan to install DII COE releases that have been approved for fielding.

DC18 PMs, to include those developing site-specific applications, shall initiate DII COE testing when each new release is approved for fielding.

New releases of segmented IMAs include:

- Major releases (i.e., an initial release or a release that changes the architecture or operation - identified by “n.0”).
- Minor releases (i.e., may contain new capabilities and features, but the fundamental architecture remains unchanged - identified by n.n).
- Maintenance releases (i.e., patch, fixes, corrects deficiencies, identified by n.n.n)

DC19 The DoDIIS Test Facility shall:

- Ensure and document that each IMA version release (i.e., major, minor, or maintenance) is compliant with these Instructions.
- Publish compliance findings according to current DoDIIS procedures and send a report to the DoDIIS SIMO for inclusion in DMB deliberations regarding a go/no go recommendation to take the configuration item to its next milestone.

3.3 APPLICATION DEVELOPMENT AND SEGMENTATION

3.3.1 Segmentation of DoDIIS IMAs

A DII COE developer’s toolkit provides all required tools to complete the segmentation process. The toolkit is available from the DoDIIS Distribution Facility with each DII COE baseline. Documentation describing the segmentation process can be found at http://spider.dii.osfl.disa.mil/cm/cm_page.html. (Note that DISA also sponsors formal training courses and seminars on the segmentation process.)

All IMA segments will be maintained in a DoDIIS Asset Repository, maintained by the DoDIIS Distribution Facility. IMA segments will be entered into the repository after being tested at the DoDIIS Test Facility and release authority has been granted. The DoDIIS Distribution Facility will manage the release of IMA segments that have been certified to field.

DC20 PMs shall:

- Deliver IMA segments, configuration definitions (where appropriate), and corresponding documentation only to the DoDIIS Test Facility.
- Refer all software distribution requests to the DoDIIS Distribution Facility.
- Obtain DoDIIS baseline software only from the DoDIIS Asset Repository.

As part of the DoDIIS segmentation process, segment descriptors and descriptor files are created. In the DII COE I&RTS, the types of descriptors and the required and optional information that is to be contained in descriptor files are identified. Some information identified as optional by DISA is required by DoDIIS and will be included in each IMA segment.

DC21 In addition to the required items shown in the DII COE I&RTS, PMs shall implement the following in each UNIX IMA segment:

- DEINSTALL, FileAttribs, COEServices, Community, PostInstall, PreInstall, Compat, Conflicts, PreMakeInst, Icons, Menus, Requires

DISA policy is to allow only one government-developed segment to perform a particular function. The sponsor of an application intended to become a part of the COE is responsible for identifying the functional requirements that are being satisfied by the application and ensuring that the application is segmented. (See Appendix E for a description of DII COE sponsorship.)

For the most part, PMs are responsible for the development of IMAs, which are not a part of the COE, but are designed to execute within a TS/SCI-certified DII COE infrastructure at each DoDIIS site. However, some PM activities are directed at the development or acquisition of common support capabilities (e.g., JDISS and Joint Intelligence Virtual Architecture (JIVA) applications). If approved by the DMB, DoDIIS organizations may sponsor common support applications for inclusion in the COE.

DC22 PMs developing DII COE common support segments shall be responsible for segmentation, documentation, and associated costs.

DC23 DoDIIS PMs that are developing DII COE common support segments shall follow the DoDIIS acquisition management process.

DC24 PMs shall identify their applications and product baseline in their APB.

3.3.2 Segment Registration

Segment registration is required for DII COE compliance. Registration is the process by which a PM registers such items as the name and ports of the segment(s) they are developing. Registration prevents naming and port conflicts with segments developed by other DoD Program Managers, allowing segments from multiple sources to peacefully co-exist on the same platform. Segment registration is one of the initial steps of the segmentation process. It is not a configuration management tool; rather it is a development tool that helps to promote interoperability. All mission (to include site-specific) and common support segments must be registered in a DISA-maintained segment registration database. See http://spider.dii.osfl.disa.mil/cm/online_db.html for instructions on how to update the DII COE segment registration database. (See the DII COE I&RTS for additional information.)

DC25 All PMs and sites shall register their respective segment(s) prefix names and applicable information in the on-line segment registration database, which can be found at http://spider.dii.osfl.disa.mil/cm/online_db.html.

3.4 DII COE I&RTS COMPLIANCE GOALS

The DoD and DoDIIS long-term objective is to achieve a highly modularized, integrated, common operating environment. Duplication of functionality, at the infrastructure, common support application, and IMA levels must be minimized. The DoDIIS long-term objective is conceptualized by level 8 compliance, as defined in the DII COE I&RTS and explained in Appendix B. At the IMA level, the DoDIIS objective can only be achieved through a functional decomposition of the IMAs, as explained in Section 3.4.2.

3.4.1 General Segmentation Considerations

Much of the present or planned functionality for IMAs is derived from the existing concept of migration systems. Considerations needed to transform an IMA (migration system) to a DII COE segmented application are discussed in the DII COE I&RTS.

DC26 PMs shall implement a migration strategy and make available requisite documentation, as outlined in the DII COE I&RTS.

DC27 PMs should use public application programming interfaces (APIs) or a COE-approved commercial off-the-shelf (COTS) API whenever possible.

3.4.2 Functional Decomposition

The DII COE defines functional capabilities for common support and infrastructure services that are generally applicable to and needed by all IMA PMs. To achieve level 8 compliance, IMAs must be designed to take maximum advantage of the DII COE common support and infrastructure services segments. The segment must not duplicate any functionality contained elsewhere in the system, whether as part of the COE or as part of another mission applications or database segment.

The DoDIIS SIMO report, *Defining a Functional Reference Model for Intelligence (FRM-I)*, describes a generic process for analyzing and decomposing intelligence mission functions (e.g., Indications and Warning, Current Intelligence, General Military Intelligence and Targeting). Using the functional matrix as a baseline, commonality among intelligence activities can be identified and developed for community use.

To realize the objectives inherent in the concept of a functional reference model, PMs will have to complete a functional decomposition of their respective IMA. After the functional decomposition of all IMAs has been completed, the DMB staff will create a functional matrix to identify commonality among the IMAs. The DMB staff will then present the results of the assessment to the community. These results will be used in the effort to define a process for achieving community-wide DII COE compliance at levels higher than level 5.

The following instructions address general requirements regarding the functional decomposition of IMAs.

- DC28** PMs shall design their application in a manner that provides for maximum (re)use of DII COE infrastructure and support segments and takes maximum advantage of reusable segments in the DoDIIS Asset Repository.
- DC29** The DoDIIS ERB and DoDIIS SIMO shall work with the DRB to develop the process to accomplish the functional decomposition of the IMAs. The process will be defined by the date specified in the DoDIIS Calendar.
- DC30** After the functional decomposition process has been defined, PMs shall accomplish the functional decomposition for their respective IMAs.
- DC31** PMs shall have their functional decomposition completed by the date specified in the DoDIIS Calendar.

3.4.3 Data Standardization/Segmentation

Policy governing the data standardization process, which is being pursued as part of the Defense Information Management (IM) Program, is documented in DOD Directive 8320.1 and the accompanying 8320.1-M Manuals. The DII COE Shared Data Engineering (SHADE) Program implements the DoD standardization policy. The primary objectives of SHADE are to promote the development of reusable off-the-shelf database segments, reduce redundancy across databases, standardize and simplify the server installation process, and promote the coexistence of independently developed databases on shared data servers. The segmentation concepts promoted by the SHADE Program provide value-added capabilities that are over and above the support standards provide in promoting database interoperability. The objective is to ensure that data element definitions and database design approaches used within DoDIIS are consistent with DoD standards.

- DC32** PMs shall review the SHADE information and compliance guidelines provided in the DII COE I&RTS and at <http://diides.ncr.disa.mil/shade/>.
- DC33** PMs shall implement the database segmentation, reuse, and data sharing concepts that are defined as an integral part of the DII COE SHADE Program.
- DC34** PMs shall comply with DoD Directive (DoDD) 8320.1.
- DC35** By the date specified in the DoDIIS Calendar, the DRB, DoDIIS SIMO, ERB, and the DoDIIS Test Facility shall use DoDD 8320.1 as a criterion for milestone progression go/no go recommendations.

As an initial step in moving to a data environment that supports the concepts of SHADE, the JIVA Management Office (JIMO) is sponsoring the JIVA Analytic Data Environment (JADE) effort. The initial implementation of JADE is expected to be the enterprise version of Broadsword. JADE will provide intelligence analysts with transparent access to several different sources of information using a single query to disparate databases using different data models.

- DC36** The JIMO shall be responsible for ensuring that its JADE initiative is consistent with the architecture constructs of DISA and NIMA and is JTA compliant.
- DC37** The JIMO shall brief the DMB on this initiative as it progresses.

3.5 GENERAL TECHNICAL GUIDANCE

3.5.1 Standards

The *DoD Joint Technical Architecture (JTA)* “mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The JTA is to be used by anyone involved in the management, development, or acquisition of new or improved systems within DoD.” Because DoDIIS is within the scope of the JTA mandate, DoDIIS PMs must use the JTA when developing DoDIIS IMAs and developing or acquiring support applications. The *DoDIIS Profile to the DoD Joint Technical Architecture and Defense Information Infrastructure Common Operating Environment* complements the DoD JTA by refining JTA guidance in some service areas and augmenting it in service areas not covered by the JTA.

DC38 PMs shall comply with the *DoD Joint Technical Architecture* and *DoDIIS Profile to the DoD Joint Technical Architecture and Defense Information Infrastructure Common Operating Environment*.

DC39 The DMB and the DoDIIS Test Facility should use JTA compliance as a criterion for milestone progression and go/no go recommendations and decisions.

3.5.2 Operating Systems

The DMB has selected two TOSs--Sun Solaris and Microsoft Windows NT, but recognizes the need for special purpose hardware and software to support imagery applications. (See *DoDIIS Profile of the DoD JTA and DII COE* for the TOS versions that are supported.)

DC40 PMs shall obtain DMB approval to use OSs other than Sun Solaris or Microsoft Windows NT on a case-by-case basis.

DC41 PMs shall continue to support legacy OS environments during the time period specified in the DoDIIS Calendar.

DC42 All DoDIIS sites shall be capable of testing with the TOSs.

DC43 All DoDIIS sites shall complete the transition to the TOSs by the date specified in the DoDIIS Calendar (for application and data servers used to house IMAs and workstation platforms used to interface with IMAs).

DC44 All applications developed to Microsoft Windows NT shall be capable of executing on any platform that supports Microsoft Windows NT.

DC45 PMs who, for performance reasons, require the use of nonstandard NT APIs, such as those available on DEC Alpha NT platforms, shall request a waiver from the DMB before a contract is let or before the Contract Renewal or Engineering Change Proposal is executed.

DC46 PMs using Windows NT COTS applications shall use only those applications that are certified under the Microsoft Logo Program.

DC47 PMs developing Windows NT-based applications should coordinate with the DoDIIS Test Facility to determine the requirements for Microsoft Logo testing.

DC48 The DoDIIS Test Facility shall perform Microsoft Logo Testing for IMAs developed to Microsoft Windows NT.

3.5.3 Support for Web and Multi-tiered Architectures

The DoDIIS long-term objective is to employ a multi-tiered architecture; the near-term objective is to employ a 3-tiered architecture.

- DC49** PMs shall provide access to data tiers through Open Database Connectivity (ODBC) transports.
- DC50** To ensure data tier platform and database engine independence, PMs shall prepare ODBC data definition language scripts and bulk data loads.
- DC51** PMs should support a web-based presentation tier designed around a vendor-neutral interface, capable of being accessed by Netscape and Explorer.
- DC52** PMs shall ensure that their use of the Hypertext Markup Language (HTML) and the Extensible Markup Language (XML) is in compliance with the standards identified in the DoD JTA.
- DC53** PMs shall use only those browser features that are supported by the standards identified in the JTA.
- DC54** PMs shall ensure that scripting, programming, and macro capabilities that are provided with the presentation tier follow appropriate JTA-specified style guidelines.
- DC55** PMs shall obtain DMB approval for browser plug-ins prior to implementation.
- DC56** PMs using plug-ins shall identify the need for the plug-ins to the DoDIIS Test Facility and ensure availability of the plug-in through a valid contract.
- DC57** Sites shall not use plug-ins downloaded from the Internet on secure networks.

3.5.4 Object-Computing Technologies

DII COE supports object-computing technologies such as Distributed Component Object Modules (DCOM) and Common Object Request Broker Architecture (CORBA). PMs may use these environments, as required.

- DC58** PMs, who use distributed object-computing solutions, shall use either DCOM or a CORBA-compliant object broker as specified by DII COE.
- DC59** PMs, who use CORBA, shall:
 - Provide a bridge to system architectures supported by DCOM.
 - Use an object request broker that has been segmented for DII COE.

3.5.5 Mobile Code

The DMB does not discourage the use of mobile code, such as Java, for IMAs. (See Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, for details regarding the definition of mobile code.) DMB policy regarding the use of mobile code is summarized in Appendix D. DMB policy is applicable to all mobile code that can be delivered across networks and executed without user intervention. The policy encourages the development of browser-neutral code so as not to require the use of a particular technology. The policy recognizes the right of each DoDIIS organization or PM to choose to implement or restrict the use of mobile code. Nothing in the policy relieves the commands, sites, or

PMs from conforming to existing DoD policies, standards, specifications, regulations, instructions, and directives, or any applicable laws.

DC60 PMs shall adhere to Director of Central Intelligence Directive (DCID) 6/3 and DMB policy regarding the use of mobile code technology.

3.5.6 Reuse

DoDIIS supports the concept of reuse among DoDIIS PMs and between DoDIIS PMs and other DoD Service and Agency PMs. The DoDIIS Asset Repository is the starting point for creating and implementing a community reuse library that the PMs can take advantage of.

DC61 PMs shall design IMA segments in a manner that maximizes their reuse potential.

3.5.7 Support for Low-Bandwidth Communications

Not all DoDIIS sites are supported by robust communications. To adequately support users interfaced through low-bandwidth communications:

DC62 PMs shall design applications with options that provide users with the capability to reduce the volume and type of information transmitted (e.g., options that allow users to turn off graphics or compress data), or implement a component-based architecture that minimizes the amount of data passed between the server and remote clients.

3.5.8 Consolidated Application Server Requirements

One of the principle concepts behind DII COE is the sharing of resources among IMAs residing on a common platform. Because all IMAs will, at a minimum, be level 5 compliant, they will be capable of peaceful coexistence on a shared platform. The added steps needed to satisfy Consolidated Application Server (CAS) requirements are characterized through the following instructions:

DC63 PMs shall not modify resources shared among all applications executing on a server.

DC64 PMs shall ensure that any planned or abnormal termination of an application does not adversely affect any other application that is executing on the same platform.

- DC65*** PMs shall not design, develop, integrate and test, or deliver IMAs intended for a 1:1 ratio, IMA to server.
- DC66*** Performance and site administration considerations shall serve as guidance for the number of IMAs that will execute on a single server platform.
- DC67*** The DMB staff and DoDIIS Test Facility shall use the CAS requirement as a criterion for a milestone progression go/no go recommendation.

SECTION 4

DODIIS TESTING AND EVALUATION

This section of the *DoDIIS Instructions* broadly outlines the guidance to the test agencies and Program Managers concerning Test and Evaluation (T&E). Test agencies and program managers can find detailed guidance in the *Test and Evaluation Policy for Department of Defense Intelligence Information System (DoDIIS) Intelligence Mission Applications (IMA)*. This document is available on the Web at

- JITF Intelink - <http://web1.rome.ic.gov:82/vtf.cgi>
- JITF Internet - http://www.if.afrl.af.mil/programs/jitf/welcome_packindex.html
- 497th Intelligence Group (IG) intranet - <http://www-act.bolling.af.mil/ind/t&edocs.htm>

Copies can also be obtained by contacting the DExA for T&E at dexat&e@emh-497ig.bolling.af.mil.

4.1 OVERVIEW

In June 1995, the Unified Commands requested that DoDIIS migration systems be certified for integration, interoperability, security, and training to ensure quality software is deployed to DoDIIS sites. In November 1995 the DMB approved the 497th IG as DExA for T&E and gave it the responsibility for oversight of the T&E portion of the DoDIIS AIS Certification Process. In June 1996, the DR/DIA approved the application of the DoDIIS Certification Process to all DoDIIS migration systems destined for installation at DoDIIS sites. In 1998, at the direction of the DMB, the terms automated information system (AIS) and migration system, when applied within the DoD Intelligence Community, were replaced with the term Intelligence Mission Application (IMA). The DoDIIS Certification Process has since been expanded to include all applications and infrastructure being installed at DoDIIS sites.

In February 1997 the Charter for the newly established Test Process Oversight Committee (TPOC) was approved and signed. The current TPOC membership is drawn from the DMB/DRB, DoDIIS SIMO, Service SIMOs, and the Director, Intelligence Systems, 497th IG with advisory input from the test agencies, user community, program managers and the DoDIIS ERB. The TPOC Membership instituted the policies that formed the basis of the *Test and Evaluation Policy* document referenced above. They continue to provide valued input as this document is revised to reflect the practicalities of the testing environment, the necessities of the users, and the philosophy and dictates of these *DoDIIS Instructions*.

T&E of IMA software releases installed at DoDIIS sites encompasses any combination or all of the following:

- Integration testing by the DoDIIS Test Facility (JITF)
- Interoperability certification testing by the Joint Interoperability Test Command (JITC). When applicable, standards conformance certification testing may be required in addition to the interoperability testing. Applicable standards identified include the National Imagery Transmission Format Standard (NITFS) and the United States Message Text Format

(USMTF).

- Security testing and certification by DIA, NIMA, or a Service security certifier agent
- Beta II testing at an operational site

The DMB membership has approved the designation of the JITF as the DoDIIS Test Facility and has given it the expanded role of ensuring IMA compliance with the *DoDIIS Instructions 2000*. This compliance verification is accomplished throughout the testing process depicted in Figure 4-1. The JITF will continue to perform installation, integration, and infrastructure compliance testing and will directly support testing by other agencies as noted above. The expanded responsibilities will be phased-in and include the following:

- Determine and document the adequacy of functional testing by IMA developers
- Identify and document duplicative functionality among IMAs or between IMA and DII COE segments. (The DMB Membership or designated agents are responsible for de-conflicting duplicative functionality.)

4.2 DODIIS TESTING AND EVALUATION POLICY

Every IMA must adhere to DoD policy and NFIP Program Manager guidance before it will be included in the DoDIIS Asset Repository. The objective of the testing process is to field IMAs that meet the requirements of users at operational sites. Test objectives to achieve a Milestone III decision by the MDA to approve fielding are itemized in the *Test and Evaluation Policy* document referenced above, and outlined in Section 2 of these Instructions. The test process will be modified to reflect the transition from the current client-server environment system services (CSE-SS) infrastructure to the DII COE and the expanded responsibilities of the JITF. The testing environment will include functionality common throughout the DoDIIS Community and as reflected in the inventory held in the DoDIIS Asset Repository. The JITF goal is to provide the attributes of a common operating environment, ensuring that IMAs will function on the infrastructure baseline.

The T&E policy, in conjunction with the DoDIIS Certification Process, ensures that fundamental quality attributes are met by each IMA. This allows individual operational sites to focus their resources on their site-unique attributes that may affect or be affected by IMAs.

TF1 The JITF shall:

- Perform compliance testing of the DII COE kernel configured for DoDIIS and segmented IMAs to determine DII COE compliance levels and verify that segments:
 - Work correctly within the COE runtime environment
 - Do not adversely affect one another
 - Conform to standards and specifications described in the DII COE I&RTS
 - Have been validated by the COE tools
 - Can be installed on top of the COE by the COE installation tools
- Identify and document IMA functional duplication for the DMB
- Test IMAs against the approved DoDIIS DII COE baseline
- Perform Logo Testing for Windows NT-based applications
- Support DoDIIS transition from CSE-SS to DII COE

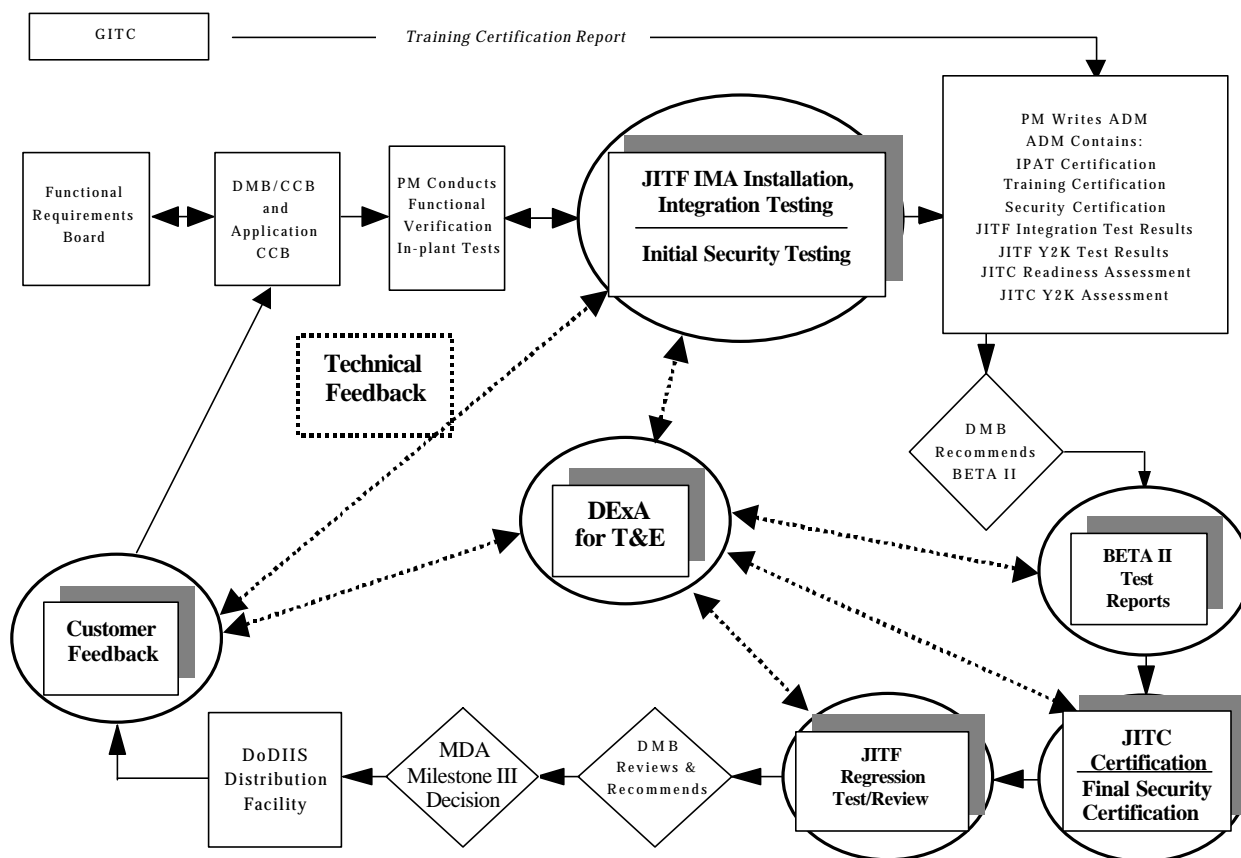


Figure 4-1. Testing and Certification Process

- Verify IMA compliance with the *DoDIIS Instructions 2000*
- Review maintenance releases of IMAs and provide the DoDIIS SIMO and DRB Chair a recommendation regarding issuance of a Certificate to Field within DoDIIS
- After a Certificate to Field has been issued for an IMA release, forward appropriate segments to the DoDIIS Asset Repository
- Directly support testing by other agencies as noted above
- Conduct Y2K integration testing in accordance with OSD directives and guidance

TF2 The JITC shall:

- Identify all DoDIIS and non-DoDIIS interfaces for each IMA.
- Perform interoperability testing and certification for each IMA with all available interfaces at the DoDIIS test facility and Beta II site. Non DoDIIS (to include Global Command and Control System [GCCS]) intelligence applications' interfaces will be tested if available at a Beta II site.
- Verify during Beta II testing that the IMA under test interoperates as needed in an operational environment with other IMAs.

TF3 Security Certifiers (Agency/Services) shall:

- Ensure each IMA meets all relevant security requirements for system operation IAW DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*.

TF4 PMs shall:

- Refer to and abide by the testing and evaluation process outlined in *Test and Evaluation Policy* document referenced in the opening paragraph, above.
- Deliver IMA segments (software) to the DoDIIS Test Facility.
- Provide complete installation documentation to the JITF in preparation for IMA testing
- Perform In-Plant Acceptance Testing (IPAT) to ensure operational readiness of the IMA with respect to satisfying functional requirements
- Provide the JITF with IPAT results prior to start of integration testing
- Ensure IMAs can be tested non-intrusively in both the legacy operating environment (until the date specified in the DoDIIS Calendar) and the objective operating environment.
- Ensure all IMAs undergo the DoDIIS Certification Process prior to installation at DoDIIS sites. The test and evaluation results will be an integral part of each IMA Milestone III ADM.
- Ensure COTS products designed and intended to function solely in an IMA environment undergo the DoDIIS Certification process, i.e., test and evaluation to verify integration and interoperability with other systems, prior to installation at DoDIIS Sites.
- Involve the user community throughout IMA development, but specifically during IPAT.

Figure 4-2 illustrates the Certification Process in terms of the DoDIIS Milestone II and III Certification Process timeline from the time of In-Plant Acceptance Testing (IPAT) through issuance of Certification to Field and can be correlated to Figure 4-1.

4.3 YEAR 2000 COMPLIANCE

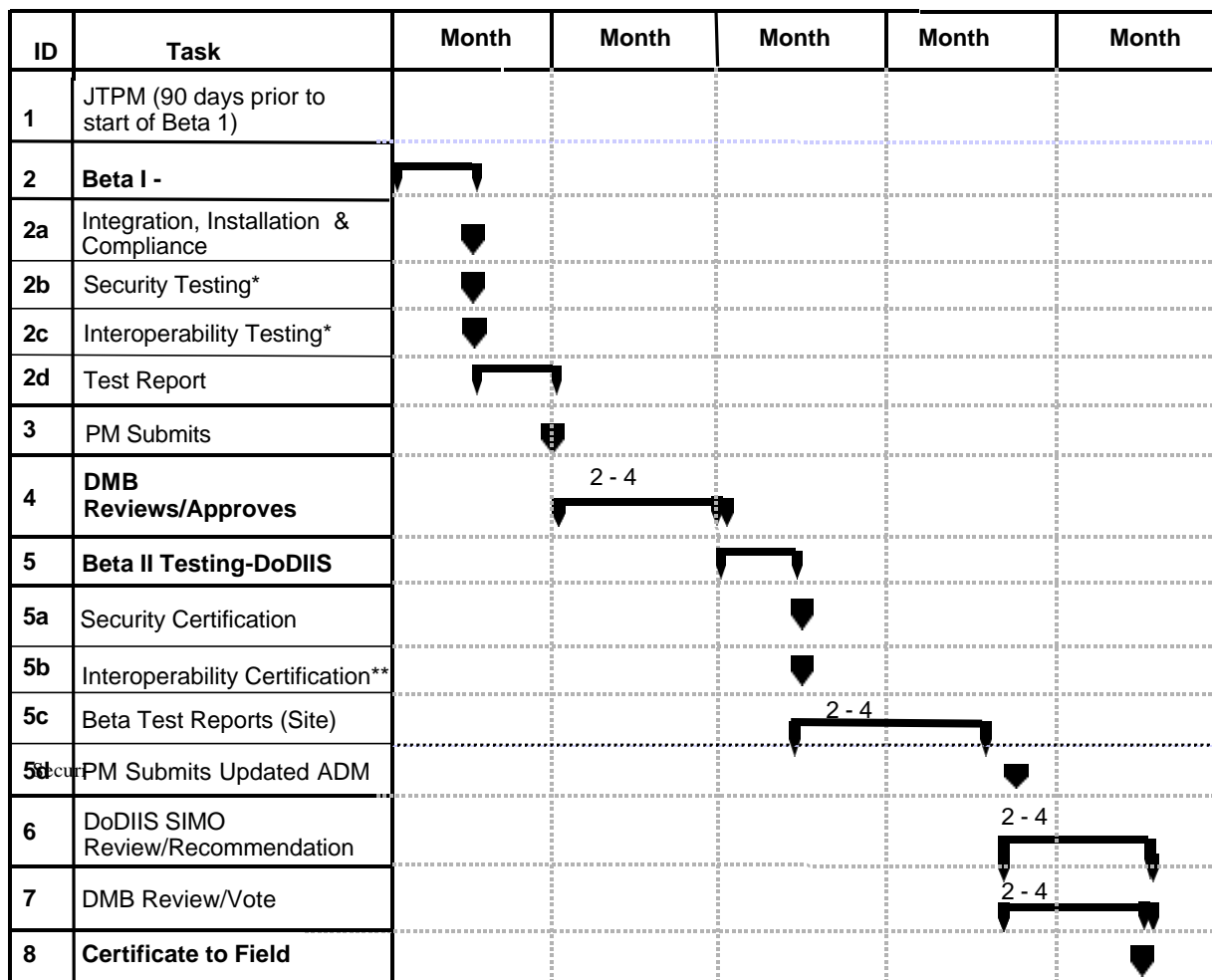
Y2K testing will continue for IMAs into 2001 as stated by OSD. The Y2K test requirements will continue until rescinded by convening authority. The Test agencies will continue to support Y2K testing as indicated above.

TF5 The PMs shall ensure that all contracts let contain a statement requiring all deliverables to be Y2K compliant as directed by the Federal Acquisition Requirements (FAR).

4.4 USER PARTICIPATION

Agency/Service SIMOs or equivalents should actively encourage IMA users in their units to become directly involved in the test process, particularly during functional testing performed during IPAT. Users can review IMA test plans and procedures for thoroughness and also are encouraged to monitor and, if possible, participate in JITF testing IAW the *Test and Evaluation Policy* document referenced above. Users should be actively encouraged to participate in Beta II testing.

DoDIIS Milestone II-III Certification Process Timeline



ADM - Acquisition Decision Memorandum DMB - DoDIIS Management Board DoDIIS - Department of Defense Intelligence Information System
 IPAT/FAT - In-Plant Acceptance Test/Factory Acceptance Test JITC - Joint Interoperability Testing Command JITF - Joint Integration Test Facility
 JTPM - Joint Test Planning Meeting * If required **If not conducted during Beta I

Figure 4-2. Testing and Certification Milestones

SECTION 5

DODIIS DISTRIBUTION

5.1 OVERVIEW

The Intelligence Community Chief Information Officer (IC CIO) of the Community Management Staff is the IC point of contact for DII COE actions. The IC CIO has tasked the JDISS JPO with the physical distribution of software releases to the Intelligence Community. In coordination with DISA, the JDISS JPO is the single point of contact for DII COE software deliveries to the Intelligence Community.

DoDIIS software assets are maintained in the DoDIIS Asset Repository at the DoDIIS Distribution Facility (DDF) at the JDISS JPO. In coordination with the PMs, Joint Integration Test Facility (JITF) and the DoDIIS SIMO, the DDF will serve as the single point of contact for Intelligence Community access to DoDIIS software assets.

5.2 DODIIS ASSET REPOSITORY

The DoDIIS Asset Repository contains the DoDIIS software inventory (e.g.: DII COE, IMAs, configuration definitions, unique DMB-approved Government off-the-shelf (GOTS) applications, and COTS products) and all related documentation. Access to untested, not yet approved assets will be restricted to DoDIIS organizations performing specific testing and certification procedures in support of the DMB. Once testing has been completed and release authority granted, the DDF extends access to DoDIIS assets to the IC community.

DF1 The DoDIIS Distribution Facility shall

- Provide the intelligence organizations of the Unified Commands, Services, and Combat Support Agencies with “one stop shopping” for DMB approved products.
- Be the single point of contact with DISA for DII COE software deliveries.
- By the dates specified in the DoDIIS Calendar, obtain DMB acceptance of the DDF concept of operations and implement the documented distribution management process.
- Coordinate license management issues with the appropriate DIA office.
- Provide an electronic software delivery capability (to include pull service).
- Maintain a DoDIIS Asset Repository that includes the software and documentation approved by the DMB for distribution.
- Interface with other DoD community distribution facilities.

DF2 The DoDIIS SIMO shall:

- Be the final authority on DoDIIS Asset Repository user account types.
- Provide the DoDIIS Distribution Facility written notification of Certificate to Field for DMB managed software assets.
- Develop and maintain a list of the current site SIMOs (or equivalent) or DRB representatives with account validation authority.

DF3 The PM shall:

- Deliver IMAs, configuration definitions (where appropriate), and corresponding documentation only to the DoDIIS Test Facility.
- Refer all software distribution requests to the DoDIIS Distribution Facility.
- Obtain DoDIIS baseline software only from the DoDIIS Asset Repository.

DF4 The DoDIIS Test Facility shall:

- Deliver DMB approved IMAs, configuration definitions, and associated documentation to the DoDIIS repository.

DF5 The site SIMOs (or equivalent) or DRB representatives shall validate DoDIIS Asset Repository account information at sites under the SIMO or DRB representative venue.

DF6 Sites shall:

- Provide the DDF with proof of purchase for vendor licensed software assets.
- Apply for access to the repository via the application form on the Electronic Asset Distribution (EAD) section of the JDISS home page.

SECTION 6

TRAINING

6.1 OVERVIEW

Training is a vital and integral part of the overall IMA acquisition process. The goal is to have training become an integral part of each IMA. To achieve this goal, training must be planned, programmed, and developed throughout the IMA acquisition. Electronic performance support systems, properly designed and integrated into the IMA, will diminish formal classroom training requirements and enhance end-user performance. The DoD General Intelligence Training System (GITS) Virtual University offers an additional training development and delivery means for IMAs. IMA training will continue to be based upon a systematic instructional system development model with focus on target audience and media analysis to ensure cost-effective training.

TR1 PMs are responsible for the training development necessary to support the IMA throughout its acquisition to include essential planning and programming actions to transfer this responsibility to a training institution.

6.2 APPROACH TO SATISFYING DODIIS TRAINING REQUIREMENTS

The DoDIIS Community will continue to rely on a combination of:

- Institutional training (i.e., DIA/JMITC, NIMA/NIMC, Service intelligence training centers, and Unified Commands to include the Regional Joint Intelligence Training Facilities).
- Technology-based performance support tools.
- Distance learning in a collaborative environment.

PMs must develop performance-based training and ensure that training is delivered to the end user in an appropriate and effective format for learning concurrent with delivery of the IMA. PMs must be proactive, budgeting and executing sufficient resources for training analysis, design and development.

TR2 PMs shall reflect training resources in their approved APB. Training development should be accomplished by professional curriculum developers concurrently with the application's development and continues through delivery and sustainment training. This is especially important in spiral and rapid prototyping efforts.

The combination of training delivery methods will be based on a training media analysis of the most cost-effective methods to deliver the initial, refresher, and sustainment training based on the user population and application complexity.

TR3 PMs shall:

- Coordinate their training planning, strategies, critical training tasks, and delivery methods with the General Intelligence Training Council (GITC) office, or Community Imagery Training Council (CITC) in a draft training management plan (TMP) prior to a milestone II decision (beginning of phase II of the development cycle).

- Coordinate the TMP with the agencies, Services, and Commands. This collaboration shall occur prior to coordination with and approval of the GITS office and prior to milestone III decision to field (during phase II of the development cycle).
- Ensure that training materials meet DoD standards and any supplementary Service standards and provide the basis for classroom and/or distant learning.

6.2.1 Institutional Training

The GITS, consisting of the DoD Components, Commands, and Services, ensures that institutional general intelligence training is effective, efficient, and responsive to intelligence training requirements. The GITS curricula include all institutional intelligence training that supports operations contained in the NFIP. Training courses have been established in such areas as special operations forces, analysis, information systems, all source collection requirements management, indications and warning, resource management, targeting, imagery, and human intelligence.

TR4 PMs shall build upon existing training programs whenever possible and coordinate their training plans with the applicable training institutions such as the DoD GITS, NIMA College, JMITC, etc.

6.2.2 Technology-Based Training

The near-term objective is to integrate IMAs into extant intelligence functional courses insofar as it is feasible within institutional or organizational constraints. Program offices must plan and program to use technology-based training as a complement and support to the DoD GITS Virtual University.

TR5 PMs shall:

- Use technology-based training as an integral part of the application development process. Training concepts should consider advanced distance learning capabilities with interactive instruction in a virtual collaborative environment.
- Employ integrated technology-based training as the primary method for delivering training for all IMAs fielded after the date specified in the DoDIIS Calendar.

The overall objective is for the user to complete applications training online, either through training embedded within the application or separate computer-based training. Based on the media analysis, training may include specific training modules or analysis/collection methodologies online with instructors or other intelligence specialists in a distance learning or collaborative environment. PMs can contact the GITS office to obtain guidance regarding the extent to which these approaches should be included in specific IMA training plans.

6.3 TRAINING MANAGEMENT PLAN

Each PM will ensure that training requirements, methodologies, and resources are identified in the TMP (Figure 6-1). All functions supported by the IMA that relate to training will be addressed in the TMP, to include functions related to the use of a unique commercial product in an IMA. Technical training for communications and computer personnel (e.g., system and database administrators), security personnel, and end user training related to applying the capabilities and features of the IMA itself must be included. The TMP is intended to be flexible and will be modified to meet PM training requirements. The IMA TMP provides a means to coordinate training resources among the materiel developers, training developers, resource managers, and users.

TR6 PMs shall:

- Ensure the TMP provides sufficient detail to support the intelligence training application, clearly showing the requirements, resource implications, and key personnel involved.
- Coordinate their TMP with, and have it approved by, the GITS office or CITC prior to Beta II testing. PMs will post the TMP on their Intelink and Intelink-S home pages.
- Update the TMP as required to reflect any changes to information therein.

6.4 TRAINING CERTIFICATION

Training certification for an IMA provides an interim review of the training process for Beta II testing and a milestone III decision to field. This approval is normally based upon successful pilot training prior to initial operating capability (IOC) and a review of training materials and courseware. The TMP provides a basis for determining if the training has been planned for and adequately resourced, with special emphasis on initial (surge) and sustainment (steady state) training. It should be noted that the program of instruction (POI) or courseware is *not* verified or validated by the GITS office. Verification and validation of training materials is accomplished during development with subject matter experts, through peer review, and during pilot training.

TR7 PMs shall ensure, through coordination with the curriculum developer and users, that the POI is verified and validated as to its content and structure.

Requests for training certification must be forwarded to the GITS office 30 working days before the milestone progression documentation is due to the DMB.

1. **Purpose.** *What is this plan attempting to accomplish? What is the scope of the program or project?*
 2. **References.** *What references are pertinent to understanding this plan and the project or intelligence mission application (IMA) involved?*
 3. **Program or IMA Planned Capabilities Description.** *Succinctly describe the training program or mission application utilization and its intended use. Include information on hardware and software that will require training—either as part of this plan or as a prerequisite.*
 4. **Training Planning Organization.** *Who is the program or project management officer (PMO)? Who is the PMO training point of contact? Who serves as the responsible training authority?*
 5. **Supporting Organizations.** *What Government and private sector (contractor) organizations are involved? Are DoD or Service intelligence schools participating? Command training facilities?*
 6. **Planning Considerations.** *Include those assumptions and facts that support the training plan.*
 - a. **Assumptions.** *Limit assumptions to those essential to support planning.*
 - b. **Facts.** *Key factors upon which training planning is based.*
 7. **Training Mission.** *Describe in general terms the overall training goal and objectives.*
 8. **Training Requirements.** *This paragraph more clearly defines the actual training requirements, skill levels, target population, etc. These should include new and critical skills, formal school training, unique training, facility requirements, location, student prerequisites/qualifications, and numbers and types to be trained--include instructors, computer specialists, communications personnel, and other support personnel. (Use enclosure, if extensive data).*
 9. **Training Execution.**
 - a. **Training concept--***What is the overall training strategy? How is "surge" or initial training handled? What is the plan for "steady state" or sustainment training?*
 - b. **Courses--***Initially, a projection of the training requirement, its subject coverage, and time, later validated and verified by analysis and design (initial estimates are useful for planning and caution is advised that these projections are revised as training developments proceeds).*
 - c. **Critical tasks--***What are the actual job task requirements? What skills, knowledge, abilities will the incumbent be required to know in performing the job? (If extensive, include at enclosure).*
 - d. **Trainers--***What types and how many trainers (primary instructors, assistants) and instructional support personnel are required for each module? For training methods other than traditional classroom lectures, is the instructor/student ratio adequate? If train-the-trainer training is required, what is the concept/method to train them? Is there an instructor certification program to ensure training instructors are appropriately qualified? If so, describe.*
 - e. **Training Administration & Scheduling--***What administration process is going to be used, e.g., plans for maintenance of training records; plans to ensure that pre-requisite courses are completed when required; plans for operation and maintenance of computer-managed-instruction software if it is used, etc?*
 10. **Organizational Responsibilities.** *Training management is a shared activity with the program/project manager responsible for the overall IMA (system) development, to include training. Support activities work within their functional roles to ensure system and training success. These include the Program Management Office, Joint Military Intelligence Training Center/DAJ, Directorate for Information Systems/DS, National Imagery and Mapping College, Services, and Commands.*
 11. **Resources.** *What funding supports the project? Is funding for training allocated? What classrooms are available? Are instructors available? What is the training force structure and cost information by fiscal year? What are the risk areas? Is there funding for sustainment training? Refresher training? How has funding been allocated in according with specific funding vehicles?*
 12. **Contacts.** *Points of contact--the budget officer, Services, Commands, etc.*
- Enclosures:** *Below are suggested enclosures to complement the basic plan; if appropriate this information may be included in the body of the plan.*
- Milestones--***if training supports an IMA, include life cycle phases reflecting TMP completion, pilot training, beta testing, and operational fielding*
- Target Audience--***population to be trained by category (military/civilian), grade/rank, occupational series*
- Critical Tasks--***perhaps the most important aspect of developing training. The identification of critical tasks supports the design and development of training by determining the learning objectives and supporting course evaluation.*
- Proposed courses--***this estimate may be a useful guide; appropriate training analysis and design is essential to define actual requirements.*
- Glossary--***include a reference of definitions and acronyms, if useful to the intended readers.*

Figure 6-1. Training Management Plan

SECTION 7

INFORMATION SYSTEMS SECURITY

7.1 OVERVIEW

Within DoDIIS, most existing security guidance is being revised or replaced to reflect the change in philosophy from risk avoidance to risk reduction and risk management. These changes also address the adoption of DoD Instruction 5200.40, *Department of Defense Information Technology Certification and Accreditation Process (DITSCAP)*, by DIA for the DoDIIS Community, and the new technical security requirements detailed in DCID 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, dated 05 June 1999.

7.2 DODIIS SECURITY CERTIFICATION PROCESS

Since the security guidance is itself under revision, the details cannot be provided here. However, the following is provided as interim guidance pending publication of the revised DoDIIS system security certification process.

SE1 PMs shall:

- Ensure the security architecture being developed for IMAs is consistent with the requirements specified in the DII COE Security Services Software Requirements Specification (SRS).
- Comply with all applicable DoD, IC, DoDIIS, and DIA security requirements, to include the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSISSS).
- Appoint a Development Security Manager for each IMA who is responsible for ensuring the system being developed is certifiable—that is, satisfies appropriate security processing requirements. In addition, the Development Security Manager is responsible for ensuring that security guidance flows from the PM to the developer and that the developer satisfies the requirements for delivering the system, to include the schedule for delivering a certifiable system.
- Comply with Office of Assistant Secretary of Defense (OASD) Memorandum, Subject: Interim Guidance for the Department of Defense (DoD) Public Key Infrastructure (PKI), ensuring only approved PKI capabilities are implemented. (See Appendix F.)
- Submit required security related documentation to the designated Certifying Organization for review and approval during the development process in accordance with the provisions of DIAM 50-4.
- Secure a review and certification by the Defense and IC Security Accreditation Team (DICAST).

SE2 In lieu of the full set of security documents described in the *Developer's Guide for Automated Information Systems Security in DoDIIS*, system security documentation shall include:

- A System Security Concept of Operations (CONOPS), which describes the purpose of the planned system, identifies all of the intended users, their clearance levels, access approvals, and need-to-know authorizations; the sensitivity of the information to be processed; system connectivity requirements; and system certification schedule. It should be written in a clear

manner that is understandable to non-technical managers.

- Security Requirements Traceability Matrix (SRTM), which includes a full description of the security requirements, the source of each requirement, a mapping of the requirement to the test procedure(s), and the method of satisfying the requirement (inspection, documentation, test, or observation). See Table 7-1 for a sample SRTM format.
- Security Test Procedures, which provide a step-by-step set of operational instructions for performing the tests identified in the SRTM.
- Trusted Facility Manual (TFM), which includes detailed information about the system's security features and procedures on how to securely configure and maintain the system.

Systems with multi-level security requirements may require additional documentation.

Table 7-1. Sample SRTM Format

REQUIREMENT	SOURCE	TEST PROCEDURE	TEST METHOD			
			I	D	T	O
All magnetic media shall have classification labels attached.	JDCSISSS	Test Case 1, Media Labeling	X			
The security features available to system users (i.e., password change, screen lock, etc) will be documented in Standard Operating Procedures or Security Features Users Guide.	DCID-Derived	Test Case 2, Documentation Review		X		
The audit data for the auditing of logon/(unsuccessful and successful) shall include: date and time, USERID, Domain system identifier (ID), workstation ID and indication of success or failure.	DII COE SRS	Test Case 3, Logon Violations			X	
The ISSO/SA shall select the privileged commands to be audited.	SYS SPEC	Test Case 4, Security Policy Changes			X	
The audit data for the auditing of the use of privileged commands (unsuccessful and successful) shall include date and time, command, security-relevant command parameters, and indication of success or failure.	DII COE SRS	Test Case5, Rights and Privileges Changes			X	
The audit data for the auditing of Discretionary Access Control (DAC) permission modification (unsuccessful and successful) shall include date and time, user (requestor) ID, user/group ID (to whom change applies) and destination, object ID, permissions requested, and indication of success or failure.	DCID	Test Case 6, Group/Account Changes			X	
All users shall demonstrate proficiency in system use.	Technical Exchange Meeting on 4/21/98	Test Case 7, User Proficiency				X

I=inspection; D=documentation review; T=test; O=observation

SECTION 8

BUDGET APPROVAL PROCESS

8.1 OVERVIEW

Section 8 complements Section 2. Section 8 is focused on the development and approval of the General Defense Intelligence Program (GDIP) budget. Section 2 discusses the milestone decision process and the roles and responsibilities of Service/Agency milestone decision authorities.

DoDIIS information systems, services, and communications are funded within the National Foreign Intelligence Program (NFIP), and, to a lesser extent, the Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA). Within the NFIP, the GDIP is the funding source for the majority of DoDIIS systems. Other NFIP components that provide resources to develop intelligence mission applications installed at DoDIIS sites include the National Imagery and Mapping Agency Program (NIMAP) and the National Security Agency (NSA) Consolidated Cryptologic Program (CCP).

8.2 GDIP BUDGET APPROVAL PROCESS

Figure 8-1 summarizes the yearly activities associated with building the President's GDIP Budget. In the November/December time frame, the DCI, Secretary of Defense and respective Program Managers issue Program Guidance (e.g., Defense Planning Guidance, Joint Planning Document, Joint Intelligence Guidance, Program Manager's Guidance Memorandum (PMGM), supplemental cost guidance) that provides direction for program development, review and justification. It is issued to the Services, Commands, and Defense Agencies. The guidance gives functional priorities and specific program guidance to follow in developing the IPOM. The GDIP PMGM provides general priorities and guidance for the program, and the DIFMs for Collection, Production and Infrastructure provide priorities and specific guidance within their functional areas. In conjunction with the PMGM, the DIFM-I issues more detailed guidance, GDIP Infrastructure Technical and Cost Guidance. Throughout the year, technical and managerial guidance is also issued by the DMB. This guidance is intended to satisfy the intelligence objectives and harmonize IMA and infrastructure development activities with site acquisition, architectures, and integration activities.

After release of the guidance, organizations, activities and projects review and prepare their IPOM submissions. In the second quarter of the fiscal year, the Commands and Component Resource Managers submit their proposed programs to the Services and DIA who review, consolidate, and prioritize their respective IPOM submissions. In April, the Services and DIA submit their IPOMs to the GDIP Resource Management Office and the DIFMs. The DIFMs, in conjunction with their program and management staffs review, consolidate, prioritize, and package the total program that will be submitted to the DCI in May for review. During the summer, the DCI and OSD staffs perform program assessments, identify and study issues, and suggest alternatives for program decisions. In August, the Expanded Defense Resources Board (EDRB) issues the IPDM. The IPDM is signed by the DCI and the Deputy Secretary of Defense (DEPSECDEF). The GDIP DIFMs incorporate these resource decisions and the GDIP Program Manager submits the Intelligence Budget Estimate Submission (IBES) to the DCI in September. After October joint budget reviews with representatives from Office of Management and Budget, the DoD Comptroller,

and the DCI Community Management Staff, the budget is finalized and incorporated into the President's Budget by December.

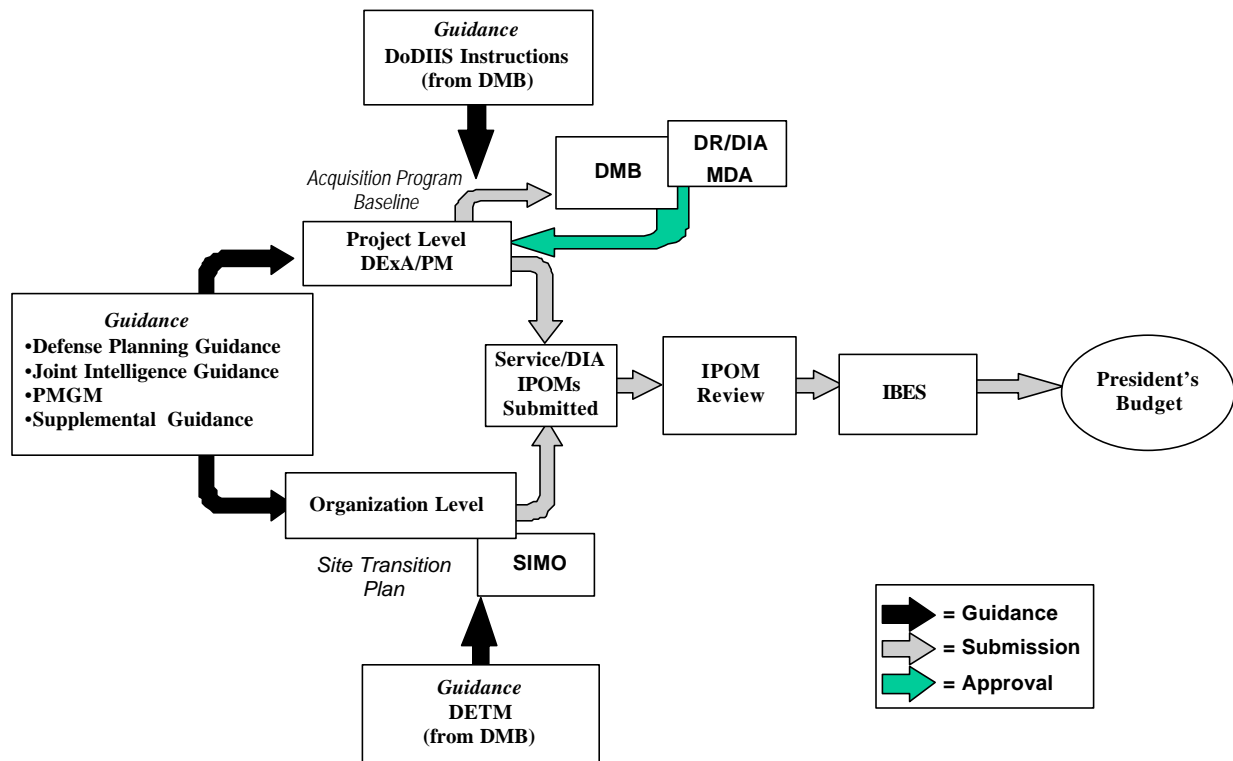


Figure 8-1. GDIP Build Process

8.3 PROJECT MANAGER GDIP RESOURCE RESPONSIBILITIES

The PM role in the resource process is to identify the cost for project development and acquisition. As required by DoD 5000.2-R (as discussed in Section 2), the initial APB is required at Milestone I and must be updated as changes occur or at each milestone review.

BUI Recognizing that project contract schedules and the Planning, Programming, and Budgeting System (PPBS) and Capabilities, Programming, and Budgeting System (CPBS) are not coincident, each PM shall update their APB each year on 1 November and post on Intelink and Intelink-S (excluding programmatic data). In that regard, the APB cost profile and the IPOM profile must match for all projects funded by the GDIP.

If the APB has changed due to a contract modification, fiscal restraints, or project re-definition it must be resubmitted for MDA approval. The changed or updated APB must have MDA approval prior to the Service and DIA IPOM submissions. The IMA must have an approved APB before the project is included into the IPOM submission. The intent is to allow sufficient time for coordination and integration of those changes into the Site Transition Plans (STP) and for DIA and

Service program build submissions. A clear linkage between IC and DoD strategic plans, Program Guidance, DoDIIS guidance and IPOM submissions needs to be established.

- BU2** PMs shall ensure that resource information (i.e. RMIS Record Number, RMIS Tier III line numbers, Format 7 and Format 9) identified in their IPOM submissions are linked to their APB.
- BU3** In the same manner, DoDIIS sites shall ensure that Program Guidance, DoDIIS Guidance and APB information are reflected in their STPs, and that the site STP and the resource information (i.e. RMIS Record Number, RMIS Tier III line numbers, Format 7's and Format 9's) identified in their IPOM submission are linked.
- BU4** Only projects with MDA-approved APBs shall be included in the Service or Agency IPOM submission. The APBs are submitted as part of the coordination process for Milestone II and III and must identify the customers, financial contributions, and any change to the project requirements.
- BU5** APBs shall reflect the current year, budget year, and five year program plans, including authorized and required funding, external funding sources, as well as an impact assessment of any stated funding shortfall, and depict the linkage between the IMA IPOM submission and the APB.
- BU6** APB updates shall reflect changes in direction regarding previously documented or planned development activities.

Changes may be brought about as a result of the program or external funding activities, because of new technological developments, or simply to react to new guidance. As a result, the APB will include costs associated with such things as:

- Satisfying user functional requirements.
 - Complying with DoDIIS technical criteria and direction.
 - Integrating DoD data standards that are currently being defined for data architectures, models, algorithms, relationships, rules, and elements.
 - Transitioning to DII COE, providing support to the COP.
 - Training.
 - Complying with Y2K specifications.
 - Migrating to DMS or sustaining existing systems until such time as DMS becomes available.
 - Satisfying interface requirements.
- BU7** The IMA budget estimates shall include direct software design, development, integration costs, facility and personnel support costs to include: costs associated with configuring and maintaining adequate software development facilities and those associated with training personnel on the use of specific types of equipment and the commercial software products that are being used in the development process.
 - BU8** The IMA budget estimates shall also include all personnel costs related to managing and completing the re-engineering effort, to include travel costs associated with attending DoDIIS Community-wide IMA management reviews and conducting design reviews and project status reviews. Cost estimates shall also include projections for maintenance.

- BU9** Throughout the development period, PMs shall monitor and control expenditures to ensure that projects remain within funding allocations.
- BU10** No later than the completion of critical design review (or equivalent), PMs shall notify sites in writing of the need to procure specialized hardware or support software, and maintenance requirements. Notification shall provide ample time for sites to program the necessary resources.
- BU11** In situations where DExAs suspect that fiscal year funding allocations are insufficient, they shall seek to rectify the situation through the appropriate Service or DIA resource component.

8.4 SERVICE/COMMAND/AGENCY SIMO RESPONSIBILITIES

- BU12** Service/Command/Agency SIMOs (or equivalent) shall assess and coordinate on the Service/Command/Agency IPOM submissions to ensure linkage between the STPs, APBs and IPOM resource information (i.e. RMIS Record Number, RMIS Tier III line numbers, Format 7's and Format 9's) submissions.

8.5 DODIIS SIMO RESPONSIBILITIES

The DoDIIS SIMO will perform an assessment of the APBs and STPs to ensure that IC, DoD, Command, Service, and Agency strategic plans, architectures and priorities are appropriately reflected.

- BU13** The DoDIIS SIMO shall develop program evaluation criteria, and coordinate the criteria with the Services, Agencies, and Commands.

8.6 RESOURCE/FUNCTIONAL MANAGERS RESPONSIBILITIES

The resource managers, working with the DoDIIS SIMOs, will review the APBs, and STPs to ensure linkage with the IPOM resource information (i.e. RMIS Record Number, Tier III line numbers, Format 7's and Format 9's) as well as compliance with intelligence guidance documents and validate project resources. The DIFMs will review the submissions to:

- Ensure compliance with DoD, NFIP, and JMIP guidance.
- Evaluate resource alternatives in consultation with the Services and Agencies.
- Identify cross-program issues with other NFIP components, the JMIP, TIARA and other government agencies.
- Ensure that the DMB and respective MDA have validated and approved the APB prior to IPOM submission.

8.7 SITE TRANSITION PLANNING RESPONSIBILITIES

DoDIIS sites are responsible for implementing the *DoDIIS Enterprise Transition Methodology* (DETM) and producing STPs.

- BU14** Each site shall:

- Perform transition-planning IAW the DETM, and reflect IC, DoD, Service, and Agency strategic planning and the C4ISR Architectural Framework. This includes developing baseline and objective systems architectures in coordination with operational and technical architectures; and planning the transition from the baseline to the objective architecture.
- Develop an annual STP IAW the DETM guidance. Specifically, the STP must support strategic planning across the DoDIIS enterprise, and support the rationalization and justification within the Command/Service/Agency IPOM submissions.

The resource managers, working with the DoDIIS SIMO, will review the STPs to ensure linkage with the IPOM resource information (i.e. RMIS Record Number, Tier III line numbers, Format 7 and Format 9).

SECTION 9

DODIIS MESSAGING

9.1 OVERVIEW

The JTA mandates the use of the DMS for both individual and organizational record messaging. DMS will eventually replace the AUTODIN, Communications Support Processor (CSP) and Newsdealer. To minimize the risks involved in scheduling and coordinating the transition to DMS, the DoDIIS ERB, in coordination with the IC DMS Management Office (ICDMO) and the IC, has developed a Transitional Messaging Architecture to support IC messaging requirements for the DoDIIS Community. The Transitional Messaging Architecture will be in existence until full IC DMS is implemented and systems employing legacy formats are converted.

9.2 TRANSITIONAL MESSAGING (i.e., AUTODIN Bypass)

DM1 The DMB Staff shall:

- Formally baseline and CM the DoDIIS transitional messaging architecture as approved by the DMB.
- Maintain a schedule of global and site transitional messaging activities.

DM2 PMs for CSP, NEWSDEALER and the Automated Message Handling System (AMHS) capabilities shall program for and sustain their messaging capabilities to support the DoDIIS transitional messaging architecture through FY2003.

DM3 Sites shall:

- Implement the approved site-specific transitional messaging architecture.
- Comply with the *DoDIIS Community AUTODIN Bypass Concept of Operation*.
- Comply with the *DoDIIS Community AUTODIN Bypass Global Routing Plan*.
- Comply with the *DoDIIS AUTODIN Bypass System (DABS) Operating Instructions*.
- Comply with the *DoDIIS AUTODIN Bypass Security Implementation Plan*.
- Program for (IPOM) and sustain their transitional messaging architecture through FY2003.

9.3 FULL DMS IMPLEMENTATION

DM4 The DMB or designate shall:

- Coordinate with the ICDMO to ensure DoDIIS DMS message-handling requirements are addressed.
- Approve/disapprove recommendations from DoDIIS DMS working groups.
- Designate an organization to provide operational management of DoDIIS DMS.

DM5 The DMB member organizations shall consolidate their DMS requirements, including tactical and SCI; provide the requirements to the ICDMO; and ensure the requisite funding requirements are identified within their respective program submissions.

DM6 PMs shall modify all applications that use AUTODIN for “data pattern” messages (e.g., Inter-Boundary Transaction Format) to use communication channels other than AUTODIN or DMS.

DM7 Sites/Services/Agencies shall:

- Program for and sustain the IC DMS architecture in their IPOM submissions.
- Comply with the *DoDIIS Community DMS System Design Architecture*.
- Identify and leverage existing resources, e.g., equipment and manpower, at all levels of the DMS hierarchy, where the architecture requires a convergence of infrastructure.
- Finalize their DMS architectures, and coordinate them with the DMB and ICDMO.
- Identify and coordinate implementation issues through the DoDIIS DMS Sites Working Group.
- Deploy DMS, to include Directory Services IAW IC schedule.

APPENDIX A

LIST OF TASKINGS

Appendix A contains a chronological, verbatim listing of all taskings. Appendix A does not add any new tasking. Additional background information and amplification regarding specific taskings can be obtained in the referenced sections.

A.1 SECTION 1—INTRODUCTION

IN1 These Instructions should be used as the basis for:

- Fiscal Years (FY) 2000 and 2001 implementation and as planning factors for the FY2002-2007 Intelligence Program Objective Memorandum (IPOM).
- Any contract awarded after approval of this document.

IN2 When there is a conflict between these Instructions and another DoDIIS document, these Instructions shall have precedence. Exceptions to this policy can be granted by the DMB.

IN3 If any instruction in this document cannot be accomplished because of insufficient fiscal resources or has negative performance, schedule, or risk impact, the affected organization shall brief the DMB and detail the impact in their FY2002-2007 IPOM using the Format 9 or Format 7 (or equivalent for DoDIIS organizations that do not use these Formats).

A.2 SECTION 2—DODIIS ACQUISITION MANAGEMENT

AC1 The DIFM-I shall:

- Implement and oversee the DoDIIS acquisition management process, to include Clinger-Cohen Act specified acquisition and system management processes.
- Review requirements at each milestone in accordance with OSD direction.

AC2 The DMB Chair shall:

- Issue a Certificate to Field for all major and minor releases (as defined in Section 3.2) of DIA IMAs, based on recommendations from the DRB/DMB.
- Coordinate on Certificates to Field for all major and minor releases of Service and Agency IMAs being fielded at more than one DoDIIS site, based on recommendations from the DRB/DMB.

AC3 The DMB shall:

- Serve as the senior joint review board for all DoDIIS acquisition management actions.
- Provide recommendations to the DMB Chair and the appropriate Service/Agency MDA concerning milestone achievement and the issuing of a Certificate to Field.
- Approve the inclusion of new software applications or tools into the DoDIIS Asset Repository, maintained by and accessible through the DoDIIS Distribution Facility (see Section 5 for added discussion of the DoDIIS Distribution Facility).
- Approve IMA software releases to be placed in the DoDIIS Asset Repository.

AC4 The DRB Chair shall review and approve or reject the recommendation from the DoDIIS Test Facility concerning maintenance releases (as defined in Section 3.2), and, if approved, issue a Certificate to Field (see Section 4 for added discussion of the DoDIIS Test Facility).

AC5 The DoDIIS SIMO shall:

- Provide recommendations to the DMB and DRB regarding milestone achievement and system readiness in support of Milestone I-III decisions.
- Coordinate with PMs to ensure adherence to DoDIIS Certification Process.

- Facilitate the day-to-day acquisition management process for the DoDIIS members.
 - Review ADM packages for relevant Milestone information, coordinate with the appropriate organizations (e.g., DoDIIS Engineering Review Board (ERB), Security, and Training), and prepare recommendations for DMB/DRB consideration.
 - Preview the recommendation from the DoDIIS Test Facility concerning maintenance releases prior to submission to the DRB Chair for approval.
 - Notify the DoDIIS Test Facility that a Certificate to Field has been issued.
- AC6** All PMs shall manage their respective software development efforts consistent with legislative, statutory and DoDIIS acquisition guidance. These Instructions include the format for preparation of an Acquisition Decision Memorandum and maintenance of a current Acquisition Program Baseline (APB) to ensure consistency with DoD 5000-series acquisition guidance (see Appendix C for the required ADM and APB format and content).
- AC7** All PMs shall validate, develop, certify and field their respective IMAs through the DoDIIS acquisition management process. This includes major, minor and maintenance releases.
- AC8** Service/Agency PMs shall coordinate their ADM for Milestones II and III with the DIA and DMB.
- AC9** DIA PMs shall have an ADM and a current, approved Acquisition Program Baseline (APB).
- AC10** All PMs shall coordinate their testing schedule through the JITF, JITC and the appropriate Security test agency.
- AC11** All PMs shall coordinate their proposed Beta II testing site(s) with the DoDIIS SIMO and the approved DoDIIS site(s).
- AC12** The DoDIIS SIMO in coordination with the IMA PMs shall review status (schedule and version development) and tailor the phases, milestones, testing requirements (coordinated with JITF) and documentation content requirements for each IMA.
- AC13** Major and minor IMA releases shall follow the full acquisition management process, resulting in a Certificate to Field.
- AC14** Maintenance releases shall be reviewed by the JITF and JITC, to determine the need for testing, and provide a 'go/no' go recommendation to the DoDIIS SIMO concerning readiness to field. PMs can appeal 'no go' recommendations to the DRB Chair.
- AC15** For DIA-developed IMAs, the ADM shall follow the complete acquisition management process, with a Certificate to Field issued upon successful completion of Milestone III.
- AC16** The DMB shall recommend to the cognizant MDA the appropriate action concerning issuing a Milestone III decision and a Service/Agency Certificate to Field.
- AC17** For Service/Agency-developed IMAs, PMs shall present the ADM to the DoDIIS SIMO for review at Milestones II and III.
- AC18** DIA PMs shall (for all Milestone decisions):
- Submit the complete ADM and approved documentation to the DoDIIS SIMO at least four weeks prior to the desired date of review/vote completion. (Sensitive situations requiring immediate processing will be accomplished in a two-week period as deemed appropriate by the DoDIIS SIMO or DMB.)
 - Brief the DMB/DRB as required.

AC19 The DoDIIS SIMO shall:

- Coordinate reviews with other organizations (to include the DRB, DIFMs, CIO, and DoD Components, as appropriate) allowing a two week period for review. (Sensitive situations requiring immediate processing will be accomplished in a one-week period as deemed appropriate by the DoDIIS SIMO or DMB.)
- Prepare a decision paper for DMB consideration. The decision paper will incorporate PM supplied data along with analysis from other sources and will cite issues that could not be resolved. Information gained in reviewing the ADM, specifically from the APB, will be used in updating the master schedule maintained by the DoDIIS SIMO. This will include dates for future Milestone decisions, tests, and version releases. The decision paper will also contain a DoDIIS SIMO recommendation regarding the ADM request.
- Execute a DMB vote, allowing a two-week review by the DMB members. (Sensitive situations requiring immediate processing will be accomplished in a one-week period as deemed appropriate by the DoDIIS SIMO or DMB.)
- Record and maintain a ballot reflecting each members vote.
- Prepare an appropriate message and letter for the Milestone and post the results of the vote on Intelink within five working days.
- Provide the DMB Milestone recommendation (or coordination for Service/Agency IMAs) to the MDA.

A.3 SECTION 3—DII COMPLIANCE GUIDANCE

DC1 The DMB shall identify the version release of DII COE that is to be used as the infrastructure baseline for the DoDIIS Community.

DC2 The DII COE version release shall undergo a security assessment to determine the current security posture of the as-released DII COE kernel with respect to use in the TS/SCI operating environment.

DC3 As required from the results of the security assessment, the DII COE kernel configured for DoDIIS shall undergo Security Certification while at the DoDIIS Test Facility.

DC4 The DMB shall approve the initial TS/SCI-certified DII COE software infrastructure baseline that is to be used at DoDIIS sites and issue a Certificate to Field.

DC5 By the date specified in the DoDIIS Calendar, every PM shall deliver IMA segments that are, at a minimum, DII COE level 5 compliant, as defined in the DII COE *Integration and Runtime Specification* (I&RTS).

DC6 Every DoDIIS site shall complete the transition of its installed computing and processing base to the DII COE standards and protocols by the date specified in the DoDIIS Calendar.

DC7 PMs developing segmented IMAs shall complete the checklist contained in the DII COE I&RTS and provide it to the DMB and the DoDIIS Test Facility with each release of their application.

DC8 PMs shall refer to the DoDIIS Asset Repository, maintained by the DoDIIS Distribution Facility, to avoid duplication of effort. The DoDIIS Asset Repository contains segments and configurations approved by the DMB for employment in DoDIIS.

DC9 The DoDIIS Test Facility shall verify the level of compliance for each segmented IMA. (See the DII COE I&RTS for more information on segment verification.)

DC10 PMs shall develop to DII COE compliant application and data servers.

DC11 PMs shall support workstation platforms that are DII COE compliant and workstation platforms that are not DII COE compliant.

- DC12** By the date specified in the DoDIIS Calendar, the PMs for the IMAs identified in IPDM I shall satisfy warfighter requirements by making, as appropriate, intelligence information available to the COP.
- DC13** PMs developing IMAs to support the COP shall support a COP interface.
- DC14** All contracts let in support of the DMB member organizations shall construct their project level priorities and deliverables taking effectivity dates into consideration.
- DC15** After Security Certification of a DMB approved TS/SCI release of the DII COE (see Section 3.1.1) has been completed at the DoDIIS Test Facility, the ERB shall lead a community effort to identify the DII COE segments that apply to DoDIIS and recommend configuration definitions (which include the DoDIIS Baseline and applicable IMAs) for DoDIIS.
- DC16** The DoDIIS Test Facility shall integrate and test each DoDIIS configuration definition upon release of each new version of the DII COE. Configuration definitions will not be fielded until a “Certificate to Field” is issued.
- DC17** All DoDIIS sites shall plan to install DII COE releases that have been approved for fielding.
- DC18** PMs, to include those developing site-specific applications, shall initiate DII COE testing when each new release is approved for fielding.
- DC19** The DoDIIS Test Facility shall:
- Ensure and document that each IMA version release (i.e., major, minor, or maintenance) is compliant with these Instructions.
 - Publish compliance findings according to current DoDIIS procedures and send a report to the DoDIIS SIMO for inclusion in DMB deliberations regarding a go/no go recommendation to take the configuration item to its next milestone.
- DC20** PMs shall:
- Deliver IMA segments, configuration definitions (where appropriate), and corresponding documentation only to the DoDIIS Test Facility.
 - Refer all software distribution requests to the DoDIIS Distribution Facility.
 - Obtain DoDIIS baseline software only from the DoDIIS Asset Repository.
- DC21** In addition to the required items shown in the DII COE I&RTS, PMs shall implement the following in each UNIX IMA segment:
- DEINSTALL, FileAttribs, COEServices, Community, PostInstall, PreInstall, Compat, Conflicts, PreMakeInst, Icons, Menus, Requires
- DC22** PMs developing DII COE common support segments shall be responsible for segmentation, documentation, and associated costs.
- DC23** DoDIIS PMs that are developing DII COE common support segments shall follow the DoDIIS acquisition management process.
- DC24** PMs shall identify their applications and product baseline in their APB.
- DC25** All PMs and sites shall register their respective segment(s) prefix names and applicable information in the on-line segment registration database, which can be found at http://spider.dii.osfl.disa.mil/cm/online_db.html.
- DC26** PMs shall implement a migration strategy and make available requisite documentation, as outlined in the DII COE I&RTS.
- DC27** PMs should use public application programming interfaces (APIs) or a COE-approved commercial off-the-shelf (COTS) API whenever possible.
- DC28** PMs shall design their application in a manner that provides for maximum (re)use of DII COE infrastructure and support segments and takes maximum advantage of reusable segments in the DoDIIS Asset Repository.

- DC29** The DoDIIS ERB and DoDIIS SIMO shall work with the DRB to develop the process to accomplish the functional decomposition of the IMAs. The process will be defined by the date specified in the DoDIIS Calendar.
- DC30** After the functional decomposition process has been defined, PMs shall accomplish the functional decomposition for their respective IMAs.
- DC31** PMs shall have their functional decomposition completed by the date specified in the DoDIIS Calendar.
- DC32** PMs shall review the SHADE information and compliance guidelines provided in the DII COE I&RTS and at <http://diides.ncr.disa.mil/shade/>.
- DC33** PMs shall implement the database segmentation, reuse, and data sharing concepts that are defined as an integral part of the DII COE SHADE Program.
- DC34** PMs shall comply with DoD Directive (DoDD) 8320.1.
- DC35** By the date specified in the DoDIIS Calendar, the DRB, DoDIIS SIMO, ERB, and the DoDIIS Test Facility shall use DoDD 8320.1 as a criterion for milestone progression go/no go recommendations.
- DC36** The JIMO shall be responsible for ensuring that its JADE initiative is consistent with the architecture constructs of DISA and NIMA and is JTA compliant.
- DC37** The JIMO shall brief the DMB on this initiative as it progresses.
- DC38** PMs shall comply with the *DoD Joint Technical Architecture* and *DoDIIS Profile to the DoD Joint Technical Architecture and Defense Information Infrastructure Common Operating Environment*.
- DC39** The DMB and the DoDIIS Test Facility should use JTA compliance as a criterion for milestone progression and go/no go recommendations and decisions.
- DC40** PMs shall obtain DMB approval to use OSs other than Sun Solaris or Microsoft Windows NT on a case-by-case basis.
- DC41** PMs shall continue to support legacy OS environments during the time period specified in the DoDIIS Calendar.
- DC42** All DoDIIS sites shall be capable of testing with the TOSs.
- DC43** All DoDIIS sites shall complete the transition to the TOSs by the date specified in the DoDIIS Calendar (for application and data servers used to house IMAs and workstation platforms used to interface with IMAs).
- DC44** All applications developed to Microsoft Windows NT shall be capable of executing on any platform that supports Microsoft Windows NT.
- DC45** PMs who, for performance reasons, require the use of nonstandard NT APIs, such as those available on DEC Alpha NT platforms, shall request a waiver from the DMB before a contract is let or before the Contract Renewal or Engineering Change Proposal is executed.
- DC46** PMs using Windows NT COTS applications shall use only those applications that are certified under the Microsoft Logo Program.
- DC47** PMs developing Windows NT-based applications should coordinate with the DoDIIS Test Facility to determine the requirements for Microsoft Logo testing.
- DC48** The DoDIIS Test Facility shall perform Microsoft Logo Testing for IMAs developed to Microsoft Windows NT.
- DC49** PMs shall provide access to data tiers through Open Database Connectivity (ODBC) transports.
- DC50** To ensure data tier platform and database engine independence, PMs shall prepare ODBC data definition language scripts and bulk data loads.

- DC51** PMs should support a web-based presentation tier designed around a vendor-neutral interface, capable of being accessed by Netscape and Explorer.
- DC52** PMs shall ensure that their use of the Hypertext Markup Language (HTML) and the Extensible Markup Language (XML) is in compliance with the standards identified in the DoD JTA.
- DC53** PMs shall use only those browser features that are supported by the standards identified in the JTA.
- DC54** PMs shall ensure that scripting, programming, and macro capabilities that are provided with the presentation tier follow appropriate JTA-specified style guidelines.
- DC55** PMs shall obtain DMB approval for browser plug-ins prior to implementation.
- DC56** PMs using plug-ins shall identify the need for the plug-ins to the DoDIIS Test Facility and ensure availability of the plug-in through a valid contract.
- DC57** Sites shall not use plug-ins downloaded from the Internet on secure networks.
- DC58** PMs, who use distributed object-computing solutions, shall use either DCOM or a CORBA-compliant object broker as specified by DII COE.
- DC59** PMs, who use CORBA, shall:
- Provide a bridge to system architectures supported by DCOM.
 - Use an object request broker that has been segmented for DII COE.
- DC60** PMs shall adhere to Director of Central Intelligence Directive (DCID) 6/3 and DMB policy regarding the use of mobile code technology.
- DC61** PMs shall design IMA segments in a manner that maximizes their reuse potential.
- DC62** PMs shall design applications with options that provide users with the capability to reduce the volume and type of information transmitted (e.g., options that allow users to turn off graphics or compress data), or implement a component-based architecture that minimizes the amount of data passed between the server and remote clients.
- DC63** PMs shall not modify resources shared among all applications executing on a server.
- DC64** PMs shall ensure that any planned or abnormal termination of an application does not adversely affect any other application that is executing on the same platform.
- DC65** PMs shall not design, develop, integrate and test, or deliver IMAs intended for a 1:1 ratio, IMA to server.
- DC66** Performance and site administration considerations shall serve as guidance for the number of IMAs that will execute on a single server platform.
- DC67** The DMB staff and DoDIIS Test Facility shall use the CAS requirement as a criterion for a milestone progression go/no go recommendation.

A.4 SECTION 4—DODIIS TESTING AND EVALUATION

TF1 The JITF shall:

- Perform compliance testing of the DII COE kernel configured for DoDIIS and segmented IMAs to determine DII COE compliance levels and verify that segments:
 - Work correctly within the COE runtime environment
 - Do not adversely affect one another
 - Conform to standards and specifications described in the DII COE I&RTS
 - Have been validated by the COE tools
 - Can be installed on top of the COE by the COE installation tools
- Identify and document IMA functional duplication for the DMB
- Test IMAs against the approved DoDIIS DII COE baseline

- Perform Logo Testing for Windows NT-based applications
- Support DoDIIS transition from CSE-SS to DII COE
- Verify IMA compliance with the *DoDIIS Instructions 2000*
- Review maintenance releases of IMAs and provide the DoDIIS SIMO and DRB Chair a recommendation regarding issuance of a Certificate to Field within DoDIIS
- After a Certificate to Field has been issued for an IMA release, forward appropriate segments to the DoDIIS Asset Repository
- Directly support testing by other agencies as noted above
- Conduct Y2K integration testing in accordance with OSD directives and guidance

TF2 The JITC shall:

- Identify all DoDIIS and non-DoDIIS interfaces for each IMA.
- Perform interoperability testing and certification for each IMA with all available interfaces at the DoDIIS test facility and Beta II site. Non DoDIIS (to include Global Command and Control System [GCCS]) interfaces will be tested if available at a Beta II site.
- Verify during Beta II testing that the IMA under test interoperates as needed in an operational environment with other IMAs.

TF3 Security Certifiers (Agency/Services) shall:

- Ensure each IMA meets all relevant security requirements for system operation IAW DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*.

TF4 PMs shall:

- Refer to and abide by the testing and evaluation process outlined in *Test and Evaluation Policy* document referenced in the opening paragraph, above.
- Deliver IMA segments (software) to the DoDIIS Test Facility.
- Provide complete installation documentation to the JITF in preparation for IMA testing
- Perform In-Plant Acceptance Testing (IPAT) to ensure operational readiness of the IMA with respect to satisfying functional requirements
- Provide the JITF with IPAT results prior to start of integration testing
- Ensure IMAs can be tested non-intrusively in both the legacy operating environment (until the date specified in the DoDIIS Calendar) and the objective operating environment.
- Ensure all IMAs undergo the DoDIIS Certification Process prior to installation at DoDIIS sites. The test and evaluation results will be an integral part of each IMA Milestone III ADM.
- Ensure COTS products designed and intended to function solely in an IMA environment undergo the DoDIIS Certification process, i.e., test and evaluation to verify integration and interoperability with other systems, prior to installation at DoDIIS Sites.
- Involve the user community throughout IMA development, but specifically during IPAT.

TF5 The PMs shall ensure that all contracts let contain a statement requiring all deliverables to be Y2K compliant as directed by the Federal Acquisition Requirements (FAR).

A.5 SECTION 5—DODIIS DISTRIBUTION

DF1 The DoDIIS Distribution Facility shall

- Provide the intelligence organizations of the Unified Commands, Services, and Combat Support Agencies with “one stop shopping” for DMB approved products.
- Be the single point of contact with DISA for DII COE software deliveries.

- By the dates specified in the DoDIIS Calendar, obtain DMB acceptance of the DDF concept of operations and implement the documented distribution management process.
- Coordinate license management issues with the appropriate DIA office.
- Provide an electronic software delivery capability (to include pull service).
- Maintain a DoDIIS Asset Repository that includes the software and documentation approved by the DMB for distribution.
- Interface with other DoD community distribution facilities.

DF2 The DoDIIS SIMO shall:

- Be the final authority on DoDIIS Asset Repository user account types.
- Provide the DoDIIS Distribution Facility written notification of Certificate to Field for DMB managed software assets.
- Develop and maintain a list of the current site SIMOs (or equivalent) or DRB representatives with account validation authority.

DF3 The PM shall:

- Deliver IMAs, configuration definitions (where appropriate), and corresponding documentation only to the DoDIIS Test Facility.
- Refer all software distribution requests to the DoDIIS Distribution Facility.
- Obtain DoDIIS baseline software only from the DoDIIS Asset Repository.

DF4 The DoDIIS Test Facility shall:

- Deliver DMB approved IMAs, configuration definitions, and associated documentation to the DoDIIS repository.

DF5 The site SIMOs (or equivalent) or DRB representatives shall validate DoDIIS Asset Repository account information at sites under the SIMO or DRB representative venue.

DF6 Sites shall:

- Provide the DDF with proof of purchase for vendor licensed software assets.
- Apply for access to the repository via the application form on the Electronic Asset Distribution (EAD) section of the JDISS home page.

A.6 SECTION 6—TRAINING

TR1 PMs are responsible for the training development necessary to support the IMA throughout its acquisition to include essential planning and programming actions to transfer this responsibility to a training institution.

TR2 PMs shall reflect training resources in their approved APB. Training development should be accomplished by professional curriculum developers concurrently with the application's development and continues through delivery and sustainment training. This is especially important in spiral and rapid prototyping efforts.

TR3 PMs shall:

- Coordinate their training planning, strategies, critical training tasks, and delivery methods with the General Intelligence Training Council (GITC) office, or Community Imagery Training Council (CITC) in a draft training management plan (TMP) prior to a milestone II decision (beginning of phase II of the development cycle).
- Coordinate the TMP with the agencies, Services, and Commands. This collaboration shall occur prior to coordination with and approval of the GITC office and prior to milestone III decision to field (during phase II of the development cycle).

- Ensure that training materials meet DoD standards and any supplementary Service standards and provide the basis for classroom and/or distant learning.
- TR4** PMs shall build upon existing training programs whenever possible and coordinate their training plans with the applicable training institutions such as the DoD GITS, NIMA College, JMITC, etc.
- TR5** PMs shall:
- Use technology-based training as an integral part of the application development process. Training concepts should consider advanced distance learning capabilities with interactive instruction in a virtual collaborative environment.
 - Employ integrated technology-based training as the primary method for delivering training for all IMAs fielded after the date specified in the DoDIIS Calendar.
- TR6** PMs shall:
- Ensure the TMP provides sufficient detail to support the intelligence training application, clearly showing the requirements, resource implications, and key personnel involved.
 - Coordinate their TMP with, and have it approved by, the GITS office or CITC prior to Beta II testing. PMs will post the TMP on their Intelink and Intelink-S home pages.
 - Update the TMP as required to reflect any changes to information therein.
- TR7** PMs shall ensure, through coordination with the curriculum developer and users, that the POI is verified and validated as to its content and structure.

A.7 SECTION 7—INFORMATION SYSTEM SECURITY

SE1 PMs shall:

- Ensure the security architecture being developed for IMAs is consistent with the requirements specified in the DII COE Security Services Software Requirements Specification (SRS).
- Comply with all applicable DoD, IC, DoDIIS, and DIA security requirements, to include the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSISSS).
- Appoint a Development Security Manager for each IMA who is responsible for ensuring the system being developed is certifiable—that is, satisfies appropriate security processing requirements. In addition, the Development Security Manager is responsible for ensuring that security guidance flows from the PM to the developer and that the developer satisfies the requirements for delivering the system, to include the schedule for delivering a certifiable system.
- Comply with Office of Assistant Secretary of Defense (OASD) Memorandum, Subject: Interim Guidance for the Department of Defense (DoD) Public Key Infrastructure (PKI), ensuring only approved PKI capabilities are implemented. (See Appendix F.)
- Submit required security related documentation to the designated Certifying Organization for review and approval during the development process in accordance with the provisions of DIAM 50-4.
- Secure a review and certification by the Defense and IC Security Accreditation Team (DICAST).

SE2 In lieu of the full set of security documents described in the *Developer's Guide for Automated Information Systems Security in DoDIIS*, system security documentation shall include:

- A System Security Concept of Operations (CONOPS), which describes the purpose of the planned system, identifies all of the intended users, their clearance levels, access approvals,

and need-to-know authorizations, the sensitivity of the information to be processed, system connectivity requirements, and system certification schedule. It should be written in a clear manner that is understandable to non-technical managers.

- Security Requirements Traceability Matrix (SRTM), which includes a full description of the security requirements, the source of each requirement, a mapping of the requirement to the test procedure(s), and the method of satisfying the requirement (inspection, documentation, test, or observation). See Table 7-1 for a sample SRTM format.
- Security Test Procedures, which provide a step-by-step set of operational instructions for performing the tests identified in the SRTM.
- Trusted Facility Manual (TFM), which includes detailed information about the system's security features and procedures on how to securely configure and maintain the system.

A.8 SECTION 8—GDIP BUDGET APPROVAL PROCESS

- BU1** Recognizing that project contract schedules and the Planning, Programming, and Budgeting System (PPBS) and Capabilities, Programming, and Budgeting System (CPBS) are not coincident, each PM shall update their APB each year on 1 November and post on Intelink and Intelink-S (excluding programmatic data). In that regard, the APB cost profile and the IPOM profile must match for all projects funded by the GDIP.
- BU2** PMs shall ensure that resource information (i.e. RMIS Record Number, RMIS Tier III line numbers, Format 7 and Format 9) identified in their IPOM submissions are linked to their APB.
- BU3** In the same manner, DoDIIS sites shall ensure that Program Guidance, DoDIIS Guidance and APB information are reflected in their STPs, and that the site STP and the resource information (i.e. RMIS Record Number, RMIS Tier III line numbers, Format 7's and Format 9's) identified in their IPOM submission are linked.
- BU4** Only projects with MDA-approved APBs shall be included in the Service or Agency IPOM submission. The APBs are submitted as part of the coordination process for Milestone II and III and must identify the customers, financial contributions, and any change to the project requirements.
- BU5** APBs shall reflect the current year, budget year, and five year program plans, including authorized and required funding, external funding sources, as well as an impact assessment of any stated funding shortfall, and depict the linkage between the IMA IPOM submission and the APB.
- BU6** APB updates shall reflect changes in direction regarding previously documented or planned development activities.
- BU7** The IMA budget estimates shall include direct software design, development, integration costs, facility and personnel support costs to include: costs associated with configuring and maintaining adequate software development facilities and those associated with training personnel on the use of specific types of equipment and the commercial software products that are being used in the development process.
- BU8** The IMA budget estimates shall also include all personnel costs related to managing and completing the re-engineering effort, to include travel costs associated with attending DoDIIS Community-wide IMA management reviews and conducting design reviews and project status reviews. Cost estimates shall also include projections for maintenance.
- BU9** Throughout the development period, PMs shall monitor and control expenditures to ensure that projects remain within funding allocations.

- BU10** No later than the completion of critical design review (or equivalent), PMs shall notify sites in writing of the need to procure specialized hardware or support software, and maintenance requirements. Notification shall provide ample time for sites to program the necessary resources.
- BU11** In situations where DExAs suspect that fiscal year funding allocations are insufficient, they shall seek to rectify the situation through the appropriate Service or DIA resource component.
- BU12** Service/Command/Agency SIMOs shall assess and coordinate on the Service/Command/Agency IPOM submissions to ensure linkage between the STPs, APBs and IPOM resource information (i.e. RMIS Record Number, RMIS Tier III line numbers, Format 7's and Format 9's) submissions.
- BU13** The DoDIIS SIMO shall develop program evaluation criteria, and coordinate the criteria with the Services, Agencies, and Commands.
- BU14** Each site shall:
- Perform transition-planning IAW the DETM, and reflect IC, DoD, Service, and Agency strategic planning and the C4ISR Architectural Framework. This includes developing baseline and objective systems architectures in coordination with operational and technical architectures; and planning the transition from the baseline to the objective architecture.
 - Develop an annual STP IAW the DETM guidance. Specifically, the STP must support strategic planning across the DoDIIS enterprise, and support the rationalization and justification within the Command/Service/Agency IPOM submissions.

A.9 SECTION 9—DODIIS MESSAGING

DM1 The DMB Staff shall:

- Formally baseline and CM the DoDIIS transitional messaging architecture as approved by the DMB.
- Maintain a schedule of global and site transitional messaging activities.

DM2 PMs for CSP, NEWSDEALER and the Automated Message Handling System (AMHS) capabilities shall program for and sustain their messaging capabilities to support the DoDIIS transitional messaging architecture through FY2003.

DM3 Sites shall:

- Implement the approved site-specific transitional messaging architecture.
- Comply with the *DoDIIS Community AUTODIN Bypass Concept of Operation*.
- Comply with the *DoDIIS Community AUTODIN Bypass Global Routing Plan*.
- Comply with the *DoDIIS AUTODIN Bypass System (DABS) Operating Instructions*.
- Comply with the *DoDIIS AUTODIN Bypass Security Implementation Plan*.
- Program for (IPOM) and sustain their transitional messaging architecture through FY2003.

DM4 The DMB or designate shall:

- Coordinate with the ICDMO to ensure DoDIIS DMS message-handling requirements are addressed.
- Approve/disapprove recommendations from DoDIIS DMS working groups.
- Designate an organization to provide operational management of DoDIIS DMS.

DM5 The DMB member organizations shall consolidate their DMS requirements, including tactical and SCI; provide the requirements to the ICDMO; and ensure the requisite funding requirements are identified within their respective program submissions.

DM6 PMs shall modify all applications that use AUTODIN for “data pattern” messages (e.g., Inter-Boundary Transaction Format) to use communication channels other than AUTODIN or DMS.

DM7 Sites/Services/Agencies shall:

- Program for and sustain the IC DMS architecture in their IPOM submissions.
- Comply with the *DoDIIS Community DMS System Design Architecture*.
- Identify and leverage existing resources, e.g., equipment and manpower, at all levels of the DMS hierarchy, where the architecture requires a convergence of infrastructure.
- Finalize their DMS architectures, and coordinate them with the DMB and ICDMO.
- Identify and coordinate implementation issues through the DoDIIS DMS Sites Working Group.
- Deploy DMS, to include Directory Services IAW IC schedule.

APPENDIX B

SUPPLEMENTAL TECHNICAL INFORMATION

Appendix B amplifies and supplements the technical information and direction contained in Section 3, DII Compliance Guidance.

B.1 DESCRIPTION OF DII COE

A thorough description of DII COE is contained in the DII COE I&RTS. Sections B.1.1 through B.1.3 provide an overview for readers who do not require the detail found in the DII COE I&RTS.

B.1.1 DII COE Layered Architecture

As shown in Figure B-1, the DII COE is made up of three layers of functionality: the DII COE Kernel, the Infrastructure Services, and the Common Support Applications. The Kernel is made up of the vendor's operating system including patches that are installed and configured per the vendor's operating instructions. The Kernel also includes segments making up the windowing system, network services such as NIS+ and DNS, COE tools, print services, basic security, system and database administration functionality, and the Executive Manager.

The Infrastructure Services and Common Support Applications are DII COE compliant commercial and government off-the-shelf (COTS and GOTS) application and support segments. These segments provide functionality in a number of areas, including: full-featured security and system administration; network administration and management; communications; message processing; message handling; office automation; mapping, charting, geodesy and imagery; help desk; collaboration; database management; Web technology (servers and browsers); distributed computing; alerts; and desktop presentation.

The DII COE COTS and GOTS segments could represent a complete application in complexity or modules equivalent to subroutines in complexity. Some segments are accessed via single mouse selection "clicks", while others are accessed by Application Programming Interfaces (APIs).

B.1.2 Building a DII COE-Based Infrastructure

Figure B-2 presents a more detailed management view of the DII COE architecture, illustrating how the DII COE common support and infrastructure segments provide a collection of building blocks that can be integrated to create a specific configuration. Ensuring that the common segments within the DII COE satisfy customer requirements is the responsibility of all organizations using the DII COE.

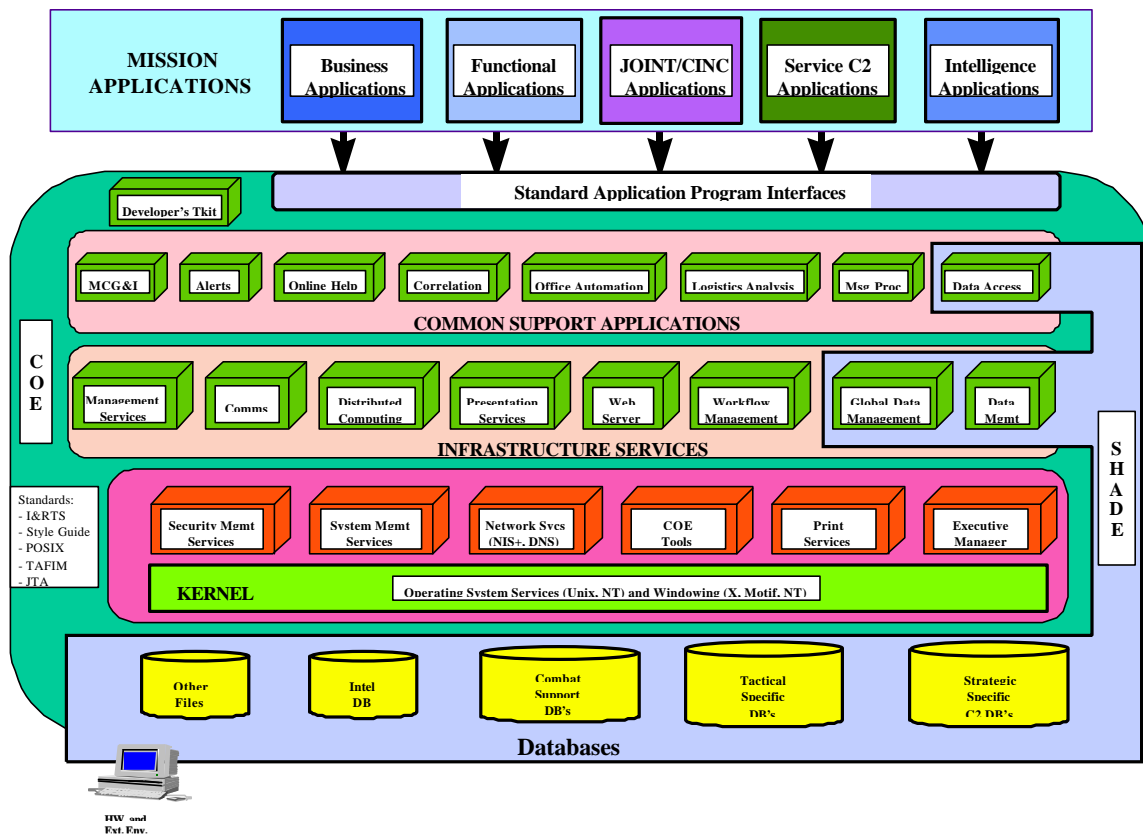


Figure B-1. DII COE Architecture

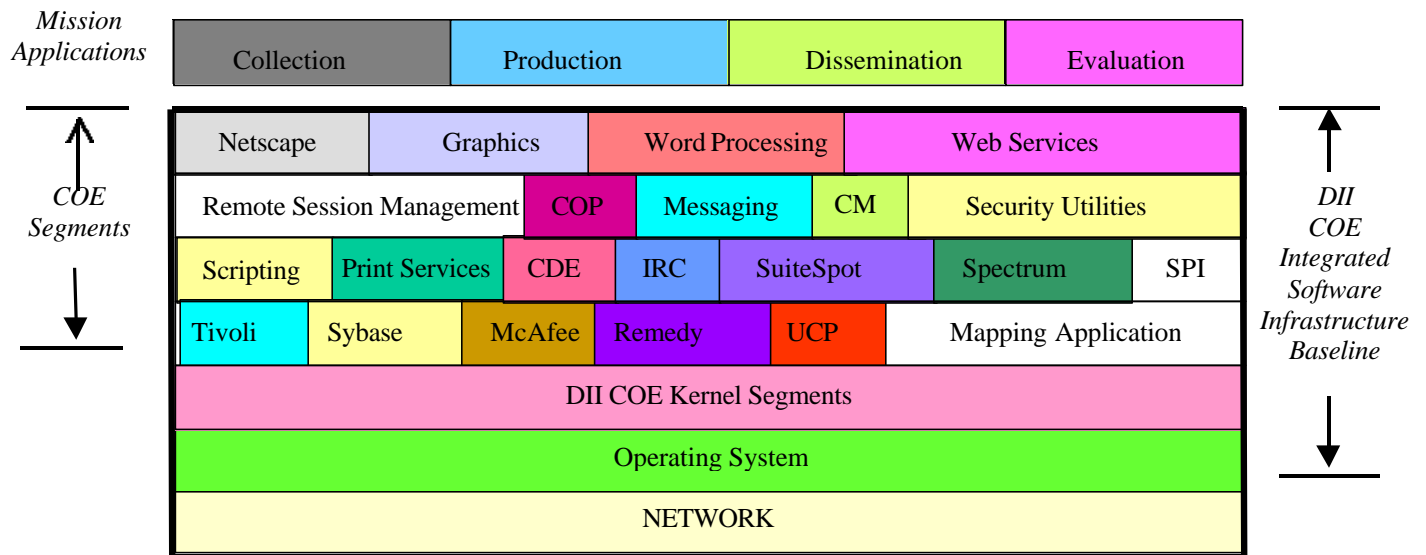


Figure B-2. Notional DoDIIS Configuration

B.1.3 DII COE Levels of Compliance

DII COE compliance is defined to be an integer value (between 1 and 8) that measures:

- The degree to which a segment or system achieves conformance with the rules, standards, and specifications identified by the COE.
- The degree to which the segment or system is suitable for integration with the DII COE reference implementation.
- The degree to which the segment or system makes use of COE services.

The DII COE I&RTS describes eight levels of compliance, but only level 5 and above (as illustrated in Figure B-3) are relevant to DoDIIS. Level 5 is the minimum acceptable level for DoDIIS IMAs; level 6 is the minimum acceptable level for all new development. To achieve level 5 compliance, entire applications, excluding database entities such as SYBASE and ORACLE data management modules, can be wrapped as a single segment. To achieve higher levels of compliance, a functional decomposition of the application is necessary, and DII COE infrastructure services and common support segments must be accessed where appropriate. Appendix B of the DII COE I&RTS contains a detailed checklist for areas where compliance is mandatory for various compliance levels.

B.2 DESCRIPTION OF THE COMMON OPERATIONAL PICTURE (COP)

The intent of the COP is to provide the Warfighter with a consistent, integrated, visual display of relevant data from all functional areas, including operations, logistics, meteorology, communications, and intelligence. The DII COE and Shared Data Engineering (SHADE) enable the COP to extract and visually present data from a wide range of local and remote sources such as field operations, information repositories, and analytical facilities of the Services and Agencies. This “view” will provide the warfighter with the resources necessary to plan, implement, and assess the effects of tactical and strategic mission objectives in the cases of global “hotspots,” limited warfare, and broad scale warfare scenarios. Details for supporting the COP are being defined by the DoDIIS Intel for the Warfighter Integrated Product Team.

“Inputs” to the COP will come from the various command and control, logistics, and intelligence organizations that participate in producing the visualization of the myriad aspects of the “total” battlespace. The vision is to provide the warfighter with the capability to “drill down” from an overarching depiction into the various layers of more and more detailed views of any specific aspect of the “total” battlespace picture.

To support the intelligence aspect of COP, designated IMAs will operate at the collateral Secret level, and will have direct access to SIPRNET. Other IMAs will provide data inputs from their respective Top Secret (TS)/Sensitive Compartmented Information (SCI) environments. These inputs will pass over the Joint Worldwide Intelligence Communications System (JWICS), through a controlled interface to the collateral Secret

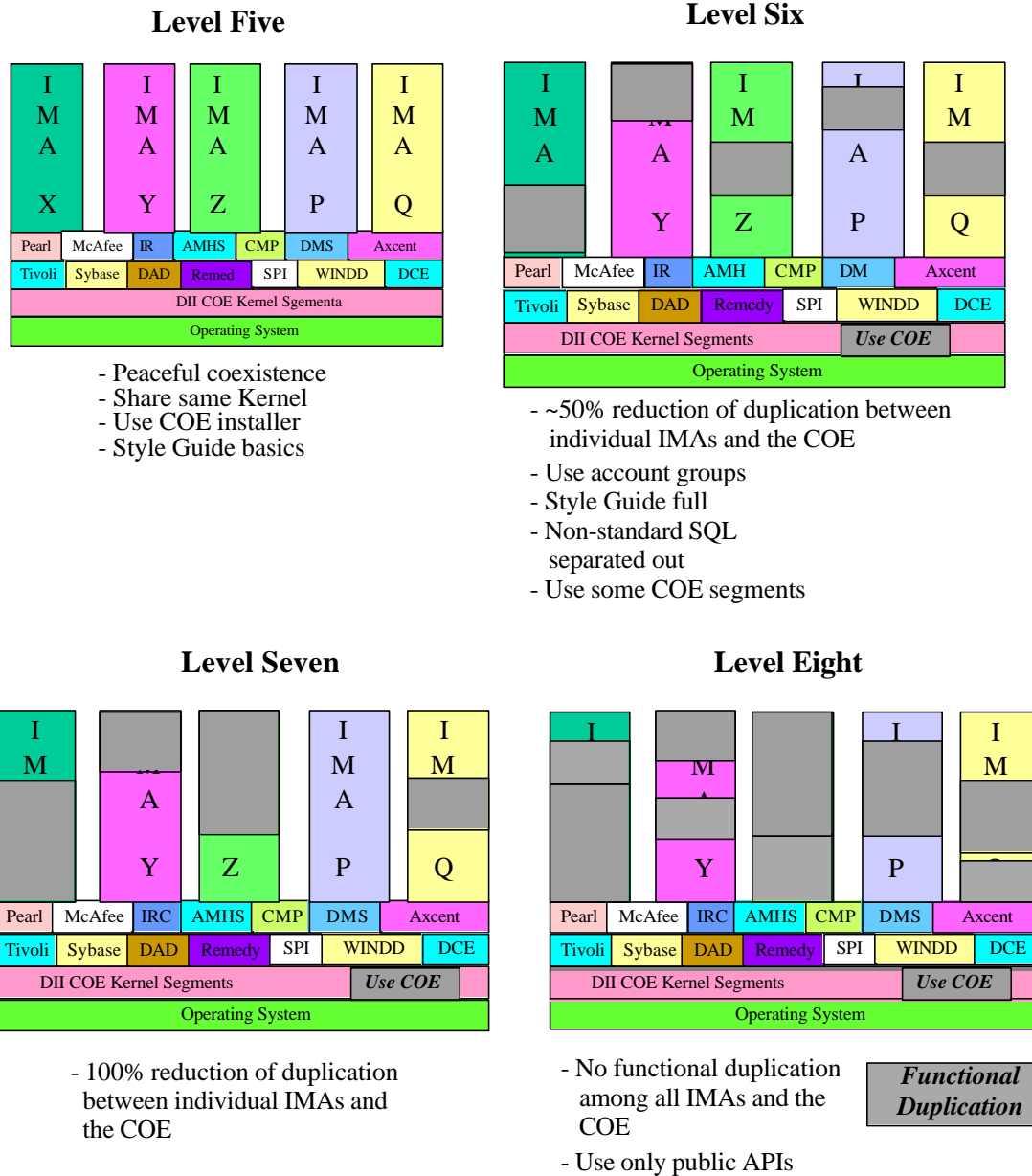


Figure B-3. DII COE Levels of Compliance

Internet Protocol Router Network (SIPRNET). For both these intelligence data sources, COP applications and tools will manipulate and process the data and display the resulting information to the warfighter. The DII COE infrastructure will provide mapping, charting, geodesy, and imagery presentation capabilities through COP applications built upon the Joint Mapping Toolkit (JMTK). Strategic and tactical intelligence databases implementing the data and structure specifications of the DII COE SHADE will enable use of a common interface for the querying and extraction of fused battle data. This fused battle data will be displayed via applications that allow the warfighter to view the battlespace from any aspect.

To standardize the intelligence interface to the COP, a DoDIIS-wide concept of operations (CONOPS) will be developed and coordinated with appropriate Joint Staff and GCCS organizations. The CONOPS will, among other things, identify how the data will be coordinated in its transfer to SIPRNET. The CONOPS will also identify the system architectures that will have to be developed to eliminate duplicative DoDIIS efforts to support the COP. As necessary, the CONOPS needs to address and clarify issues such as the following:

- How IMAs needed to provide data inputs to the COP will be identified.
- The organizations that will provide (and how many) the controlled interfaces to the collateral SIPRNET (and where will they reside).
- Which IMAs will have direct access to SIPRNET.
- When intelligence information should be provided via Intelink-S servers and how/when IMA servers should provide the data to the Warfighters.
- How information from the agencies (DIA, CIA, NSA, NIMA, etc.) will be coordinated and deconflicted from the information available from the unified commands and other “sites.”
- What working group or committee will work the issues associated with standardizing intelligence inputs to the COP.

B.3 DOD JOINT TECHNICAL ARCHITECTURE

The DoD JTA mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. A foremost objective of the DoD JTA is to improve and facilitate the ability of DoD systems to support joint and combined operations in an overall investment strategy. The DoD JTA:

- Provides the foundation for interoperability among all tactical, strategic, and combat support systems.
- Mandates interoperability standards and guidelines for system development and acquisition that will facilitate joint and coalition force operations. These standards are to be applied in concert with DoD standards reform.
- Communicates to industry DoD’s intent to consider open-systems products and implementations.
- Acknowledges the direction of industry’s standards-based development.

The JTA is to be used by anyone involved in the management, development, or acquisition of new or improved systems within DoD. Specific guidance for implementing the JTA is provided in the separate DoD Component JTA implementation plans. Operational requirements developers must be cognizant of the JTA in developing requirements and functional descriptions. System developers must use the JTA to facilitate the achievement of interoperability for new and upgraded systems (and the interfaces to such systems). System integrators must use it to foster the integration of existing and new systems. The DoD JTA can be found at <http://www-jta.itsi.disa.mil/>.

APPENDIX C

DODIIS LIFE CYCLE MANAGEMENT DOCUMENTATION

C.1 REQUIRED DOCUMENTS FOR EACH MILESTONE

Documentation requirements for each phase of the software development cycle are identified in Table C-1 and in Sections C.1.1 through C.1.4.

Table C-1. DoDIIS Documentation Requirements

Information	Milestones				Comments
	0	I	II	III	
Mission Needs Statement	X				
Operational Requirements Document		X	X	X	Update as needed
Acquisition Decision Memorandum		X	X	X	Milestone I-III
Acquisition Program Baseline		X	X	X	Update each phase as needed
Acquisition Strategy		X	X	X	Update each phase as needed
Certificate to Field <ul style="list-style-type: none"> • Interoperability Certification • Integration/Compliance Testing • Security Certification • Training Certification 				X	JITC JITF Appropriate Agencies GITC, NIMA College, etc.
Configuration Management Plan		X	X	X	Update each phase as needed
CAIV (Cost information part of APB)		X	X	X	Update each phase as needed
Security Documentation		X	X	X	Update as needed
System Documentation			X	X	ISO equivalent
Test Plan			X	X	Update as needed
Training Management Plan		X	X	X	Update as needed

C.1.1 Preparation for Milestone 0

All DoDIIS IMAs will be based on identified and validated mission needs documented in a Mission Needs Statement (MNS). Refer to Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, Requirements Generation System, 10 August 1999 for the MNS format. The MNS is prepared by the user community to document deficiencies in current capabilities and identify opportunities for new capabilities. The MNS is validated through the Joint Requirements Oversight Council (JROC) process IAW the Requirements Generation Systems. Milestone 0 is achieved when the Component Acquisition Executive (e.g., Director, DIA) approves the MNS and designates an MDA. The DoD Component will forward a copy of the draft MNS to the DMB for review. The life cycle management process begins with a favorable Milestone 0 decision and the selection of an MDA.

C.1.2 Preparation for Milestone I

The following documentation must be developed during the Concept Exploration phase and provided as attachments to the ADM:

C.1.2.1 Operational Requirements Document

The Operational Requirement Document (ORD), developed by the user or user's representative, will be used to baseline the functional requirements and identify the Key Performance Parameters (KPPs). This document will be used later in the Life Cycle Management process to identify segments for inclusion in the DoDIIS Asset Repository. Users must also develop a CONOPS to satisfy the ORD. The ORD must be validated and approved through the JROC process for a program to proceed. Refer to Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, Requirements Generation System, 10 August 1999 for the ORD format.

C.1.2.2 Acquisition Program Baseline

The PM will develop an APB to document cost, schedule and the thresholds and objective performance requirements (the KPPs from the ORD). This document serves as a contract between the PM and the MDA and is signed by both at each modification of the document. These signatures must be present when the APB is presented to the DMB. While the project remains in phase 0, the APB will be reviewed for accuracy at the beginning of each FY. Schedule information will be updated as necessary and include program initiation, major milestone decision points, initial operating capability, and any other critical system development events. An APB format is provided in Section C.2.

C.1.2.3 Acquisition Strategy

The PM must develop an acquisition strategy. The strategy is approved by the MDA at Milestone I, and updated whenever there is a change in strategy or elements of the system. At a minimum, the strategy will be reviewed for currency at the beginning of each fiscal year (see Section 8). A primary goal of an acquisition strategy is to minimize the time and cost of satisfying an identified, validated need or set of requirements. Over time the acquisition strategy evolves and becomes increasingly more definitive in identifying and describing the acquisition of essential elements of a DoDIIS system capability.

C.1.2.4 Cost as an Independent Variable

For DoDIIS IMAs, a Cost as an Independent Variable (CAIV) analysis will be developed in Phase 0 and updated throughout the life cycle management process. For an Acquisition Category III (ACAT III) program, the GDIP funding profile that includes a life cycle Cost Estimate should be developed and updated throughout the life cycle of the program. If validated functional requirements cannot be accomplished within established resources, a CAIV analysis should be developed. The relevant cost information must be included in the APB.

C.1.2.5 Risk Management

Each PM must establish and document a risk management program. The risk management program identifies, tracks, and controls performance, schedule, and cost risks; defines risk abatement plans; and provides for continuous risk assessment throughout the life-cycle process. Risk reduction measures are defined and related to cost-performance tradeoffs, as applicable. Backup or fallback strategies are described in areas of high risk.

C.1.2.6 Configuration Management Plan

An IMA-specific CM Plan, consistent with the DoDIIS CM process, must be developed to define the program CM process for controlling new software releases and maintaining operational software. See MIL-STD-973 for a CM Plan format. Each PM must ensure that the developer implements an internal CM system for the control of all documentation and software releases. This plan must address the evolving developmental configuration and support environments (e.g., engineering, implementation, and test environments) used to generate and test the product internally.

C.1.2.7 Exit Criteria

As a general rule, exit criteria are selected by the PM and approved by the MDA to track progress in key technical, schedule and risk management areas. Exit criteria demonstrate the satisfactory progress of the program. The criteria can include achieving a level of demonstrated performance, process improvement or efficiency, and/or accomplishment (e.g., system design, contract award, Certificate to Field). The proposed exit criteria must be included with the ADM.

C.1.3 Preparation for Milestone II

As appropriate, the ADM should have the following documents as attachments:

C.1.3.1 ORD

No need to resubmit this document unless change pages have been issued. Only the change pages need to be attached.

C.1.3.2 APB

This document must be amended to reflect the current performance parameters, schedule and costs just prior to submitting the ADM.

C.1.3.3 Acquisition Strategy

For applications already in the DoDIIS Asset Repository, only change pages have to be submitted. If a new development is entering the process at this milestone, the complete Acquisition Strategy shall be presented.

C.1.3.4 Configuration Management Plan

The final CM Plan must be attached.

C.1.3.5 Risk Management Plan

Only change pages need to be attached.

C.1.3.6 Security Documentation

The documentation required is described in Section 7 of the *DoDIIS Instructions*.

C.1.3.7 Training Documentation

The documentation required is described in Section 6. The Training Management Plan addresses functions supported by the system, which relate to training.

C.1.3.8 System Documentation

There is a minimum list to be presented:

- Requirements Traceability – either through a matrix, the Interface Requirements Specification or a Version Description Document (at this point the requirements specified are compared with the Acquisition Strategy and the KPPs in the APB to ensure accuracy and adequacy of the design).
- Test Plan – draft test plan, providing the approach and the success criteria (Section 4 of the *DoDIIS Instructions* provides guidelines for the preparation of this document, which will continue to evolve throughout the development phase).
- System Architecture – the proposed architecture, subject to change as the development progresses, but necessary for site planning.
- System Design documentation - no specific format for this information is required; however, the design must be clearly delineated.

C.1.3.9 Exit Criteria

The proposed exit criteria provide the factors that indicate that the next phase has met its defined goals.

C.1.4 Preparation for Milestone III

The ADM should have the following documents as attachments:

C.1.4.1 Interim Milestone III

To proceed to Beta II testing the following documents are ADM attachments:

- Acquisition Program Baseline (APB) - updated to reflect decisions made throughout the development phase.
- Acquisition Strategy - change pages only.
- The Test Report for the integration testing from the JITF and the certificate from the PM confirming successful In-Plant-Testing. For non-DoDIIS systems, the integration testing may not have been performed by the JITF; for those systems, the test plan and the report submitted IAW Section 4 of these Instructions.
- Test certification assuring successful interoperability testing.

- Security Certification - an interim certification at a minimum (for non-DoDIIS systems, the DoDIIS security personnel should review the certification for compliance and compatibility with their standards).
- Training Certification - a certificate issued by the General Intelligence Training System Office.

C.1.4.2 For the Milestone III Decision

For the ADM resulting in the Director/DIA issuing or recommending a Certificate to Field the following documents are attachments:

- The documentation listed for the interim Milestone III decision.
- Test Reports from the Beta II testing or from the users; the format for these reports can be found in Appendix C of the Test and Evaluation Policy. Message traffic is acceptable.

C.2 ACQUISITION PROGRAM BASELINE FORMAT

ACQUISITION PROGRAM BASELINE	
SYSTEM NAME	
The Acquisition Program Baseline Agreement (APB) identifies the most important key performance, schedule, and cost agreements that are the basis for satisfying identified mission needs for mission and legacy Automated Information Systems. The baseline document is a summary and does not provide detailed requirements or content.	
A general description of the system should be placed here.	
Program Director	Date
Program Executive Officer	Date
Component Acquisition Executive	Date
Milestone Decision Authority (MDA)	Date
IMA Name	
Acquisition Program Baseline	
REFERENCE:	
Mission Need Statement (MNS)	
Operation Requirements Document (ORD)	
Other Documents as Applicable	
SECTION A: PERFORMANCE	
The most important parameters are those that, if the thresholds are not met the MDA	

would require a reevaluation of alternative concepts or design approaches. These parameters evolve as the program is better defined. The number of parameters should be kept at a minimum but include those described in the ORD (the Key Performance Parameters) and validated by the Joint Requirement Oversight Council (JROC). See Paragraphs 2.3, 3.2.1, 3.2.2, 3.2.2.1 and 3.2.2.2 in DoD Regulation 5000.2-R and CJCSI 3170.01A for clarification.

PROPOSED BASELINE
Objective

PROPOSED BASELINE
Threshold

Key Parameters:

SECTION B: SCHEDULE

The following section outlines the acquisition schedule, to include initiation, major milestone decision points, initial operating capability and any other critical events (proposed by the Program Manager and approved by the MDA). Provide dates for initiation, contract activity, milestone decision points, scheduled test dates and release timelines for all anticipated versions.

PROPOSED BASELINE
Objective

PROPOSED BASELINE
Threshold

Key Events:

SECTION C: FINANCIAL PROFILE

Short Title:

Office of Primary Responsibility: Office Symbol, Mailing Address

Program Manager:

Phone Number:

Email Address:

Fax Number:

MDA I or III: (Milestone Decision Authority)

MDA Name:

Is this an update:_____

Funding Source(s): (Ex: GDIP, JMIP, CCP, TIARA,MFP-II)

Other Funding:

Is this a jointly funded or community-wide investment?

Yes _____ Service/Agency and program(s) funded

No

Mission Based Budgeting (MBB) Category: Check with your Resource Office.

Program Code: Every funded program is assigned a code; see your Resource Office.

Program Element: Check with your Resource Office.

Expenditure Center: Check with your Resource Office.

Expenditure Unit: Check with your Resource Office.

Base/On-going/New Initiative:

Program Description: Provide the mission requirement that created this program, Information Technology (IT) solution that will be applied, specific functionality that the system provides.

Customers (include internal as well as external):

Cost Benefit Analysis: Provide the expected Return on Investment,
ROI= Return/Investment Cost

Required Resources: Provide the Tier III Line Number(s) for each area by yea

Current Year	Budget Year	Program Years
00	01	02 03 04 05 06 07

RDTE: \$\$/MP

PROC: \$\$/MP

O&M: \$\$/MP

External Assistance: This should address Y2K and DII COE requirements

Systems Engineering

Integration

Development

Sustainment

Facilities:

Maintenance:

Hardware

Software

Supplies:

Travel:

Conferences/Meetings

Testing

Reviews

Installation

Training

Funding Source(s): (GDIP, JMIP, TIARA, MPF-11)
--

Resource Shortfalls (if any):

Provide Tier III Line Numbers for each area.

Current year	Budget Year	Program Years					
00	01	02	03	04	05	06	07

RDTE:

PROC:

O&M:

External Assistance: This should address Y2K and DII COE requirements

Systems Engineering

Integration

Development

Sustainment

Facilities:

Maintenance:

Hardware

Software

Supplies:

Travel:

Conferences/Meetings

Testing

Reviews

Installation

Training:

Impact Assessment: Provide functional impact statement if partially funded. State specifically which system capabilities will not be met due to funding shortfall, budget cuts or external influences.

Program Changes: Provide rationale for any funding variations since your last program build and/or APB submission.

Identify Site Architecture Requirements

Figure C-1. Acquisition Program Baseline Format

C.3 ADM FORMAT AND CONTENT

MDA approval, conditional approval, or recommendation is obtained using the ADM. The ADM is a synopsis of events (plus necessary attachments) which references program status with appropriate program and system documentation.

The following figures reflect the format and content of a Milestone I-II and a Milestone III ADM, respectively.

Office symbol	
Acquisition Decision Memorandum-- <i>Migration application name and version #</i>	
Ref:	DODIIS Instructions
To:	DMB
1.	Requested Action: Specify MDA action being requested by the PM.
2.	Project Description:
a.	General Information: Describe the project and the developmental approach (Grand Design, Incremental, Evolutionary). Discuss significant issues affecting the project design.
b.	Operational Requirements: Summarize the functional requirements that are to be satisfied by the system, identify the origin of these requirements (e.g., MNS, ORD) and identify the intended user community (at the most appropriate organizational levels).
c.	Documentation Completed: Include a summary of the system documentation that has been completed.
d.	Documentation Being Developed: Include a summary of the documentation currently being developed and expected date of completion.
e.	Training: Summarize training approach and identify user population.
f.	Interfaces: Summarize the system interfaces that will affect fielding.
3.	Proposed Exit Criteria: Include specific exit criteria to track progress in key technical, schedule and risk management areas.
4.	Point of Contact: Include name, organization, e-mail address, mailing address, phone number, and FAX number.
encls	Signature
APB	
Acquisition Strategy	
Others as appropriate	

Figure C-2. Acquisition Decision Memorandum for Milestones I-II

Office symbol	
Acquisition Decision Memorandum-- <i>Migration application name and version #</i>	
Ref:	DODIIS Instructions
To:	DMB
1.	Requested Action: Specify MDA action being requested by the PM.
2.	Project Description: Describe the migration system, identify the functional and technical management oversight forums, and identify the program manager. Details should be included as attachments.
a.	General Information: Include general project information to include description, developmental approach (Grand Design, Incremental, Evolutionary), and project documentation.
b.	Testing and Evaluation Summary: Include a summary of functional, technical, and operational testing. Identify critical/major functional, technical, operations findings and PM actions taken or being taken to correct identified problems. Test reports should be attached.
c.	Security Certification Testing: Include a summary of system security test findings. Identify Category I, II, and III deficiencies and PMO actions taken or being taken to correct the deficiencies. A copy of the System Security Certification should also be attached.
d.	Training: Include the results of the JMITC assessment and identify actions taken or being taken to correct deficiencies.
e.	Fielding: Summarize the deployment schedule and attach a detailed schedule.
3.	Outstanding Issues: Identify other issues that may impact the overall project and its schedule; discuss PM actions to mitigate risk or resolve the issues.
4.	Point of Contact: Include name, organization, e-mail address, mailing address, phone number, and FAX number.
	encls
	Certificates
	APB
	Acquisition Strategy
	Signature

Figure C-3. Acquisition Decision Memorandum for Milestone III

PM's Checklist

Required Activity	Action/Duration	Responsible Party	Date Accomplished	Mark Completed	Pending Due To:
Preparation for Milestone 0					
Mission Needs Statement (MNS), Concept Exploration (see CJCSI 3170.01A for format)		User Community			
JROC VALIDates MNS					
MNS Approved and Milestone Decision Authority (MDA) Named		Component Acquisition Exec			
<i>Milestone 0 Achieved</i>					
Preparation for Milestone 1					
Develop Documentation		Program Manager			
Operational Requirements Document (see CJCSI 3170.01A for format)		User or User's Representative			
Acquisition Program Baseline (see DoDIIS Instructions for Format)		Program Manager			
Develop Acquisition Strategy		Program Manager			
Establish and Document a Risk Management Program		Program Manager			
Develop and Define a Configuration Management Plan (see MIL-STD-973 for Format)		Program Manager			
DMB Coordination Required - PM determines in conjunction with JITF and DMB		Program Manager			
Milestone I ADM with Documents		MDA			
MDA Milestone I Decision (Begin Acquisition Program)		MDA and DMB			

Preparation for Milestone II					
Update Milestone I Documentation		Program Manager			
Schedule Joint Test Planning Meeting (JTPM) NLT 90 days prior to planned test start date		Program Manager			
Prepare Required Security Documentation (see DoDIIS Instructions Sec 7)		Program Manager			
Satisfy Training Requirements		Program Manager			
Ensure Training Resources Requirements are Reflected in APB					
Develop Training Management Plan; Post TMP on Intelink/Intelink-S					
Coordinate with General Intelligence Training System (GITS)					
Request GITS or NIMA College Training Certification 30 Days Prior to Seeking Milestone Progression		Program Manager			
Complete System Documentation		Program Manager			
Requirements Traceability (Matrix, Interface Reqs Specs, or VDD)					
Draft Test Plan (see Sec 4, DoDIIS Instructions)					
System Architecture					
System Design Documentation					
Milestone II ADM with Documents		MDA			
Milestone II ADM forwarded to DMB		Program Manager			
Information Briefing to DMB or Technical Review Board					

MDA Milestone II Decision (Enter Development)		MDA and DMB			
		As Appointed			
Preparation for Interim Milestone III					
Schedule Joint Test Planning Meeting (JTPM) NLT 90 days prior to planned test start date		Program Manager			
Factory Acceptance Testing scheduled		Program Manager			
JITF Testing scheduled		MDA or Designee			
Security Certification Testing scheduled		Program Manager			
JITC Integration Testing Scheduled		Program Manager & JITF			
NITFS Compliance Testing scheduled		Program Manager and JITC			
Beta II Site selection		Program Manager			
Beta II Testing Schedule		Program Manager & Site			
Beta II Test Plan delivered to Beta II Site detailing critical issues, and Success Criteria		Program Manager			
JITF Work Plan received by PMO return NLT 60 days to start test date		Program Manager			
Joint Test Planning Meeting at the Beta II site (JTPM) (60-90 days prior to testing):		Program Manager & Site			
PMO returns JITF Work Plan to JITF 60 days prior to Beta-I test		Program Manager			

PMO delivers system documentation to JITF NLT 30 days prior to test		Program Manager			
Requirements Definition Documentation					
Requirements Traceability Matrix					
Security Accreditation Documentation					
Test Plans, Procedures, and Test Reports					
Interface Control Document					
Software Version Description					
User Documentation					
Run Time Interface Document					
Configuration and Installation Guide					
Transition Plans					
Open Problem Reports					
PMO issues Factory Acceptance Test Certification		Program Manager			
All Cat 1 and Cat 2 Findings are closed prior to requesting auth to proceed to Beta II:					
All Cat 3 Findings are scheduled for Disposition:		Program Manager			
PMO delivers software to JITF NLT 14 days prior to test		Program Manager			
Joint Test Readiness Review (JTRR) NLT 14 days prior to JITF testing		Program Manager & JITF			
JITF Integration Testing:		JITF			
1. Draft Report delivered 5 working days after testing completion		JITF			
2. PMO has 2 days to respond to the Draft Report:		Program Manager			
3. Final Report delivered 10 days after testing completion		JITF			

4. All JITF Cat 1 Findings corrected:		Program Manager			
5. All JITF Cat 1 Findings retested/validated by the JITF:		JITF			
6. All other findings Cat 2/3 "Requiring Resolution" scheduled for work-off:		Program Manager			
Security Certification:		Security			
Test Report and Letter prepared		Security			
Security Certification Letter staffed and signed		Security			
JITC Interoperability Certification:		JITC			
1. Draft Report delivered 14 days after testing completion		JITC			
2. PMO has 3-4 days to respond to the Draft Report:		JITC			
3. JITC Joint Interop Cert and Final Test Report delivered NLT 30 days after JITC Beta II test completion		JITC			
4. JITC Y2K Assessment Letter delivered within seven days of Y2K interoperability testing		JITC			
5. All JITC Cat 1 Findings corrected:		Program Manager			
6. All JITC Cat 1 Findings retested/validated as corrected by the JITC:		JITC			
7. All other findings Cat 2/3 "Requiring Resolution" scheduled for work-off:		Program Manager			
NITFS Compliance Certification		JITC			
ADM submission Requesting Authorization to Proceed to Beta II; includes:					
FAT Testing Report with all Cat 1 & 2 Findings closed		Program Manager			

JITF Integration Test Rpt and recommendation to proceed to Beta II with any/all Cat 1 findings corrected		Program Manager			
JITC Interop Test Rpt and recommendation (if JITC testing done during Beta I)		Program Manager			
Security Certification Letter		Program Manager			
Training Certification issued by the GITC		Program Manager/Security			
Status Update Briefing to DMB to proceed to Beta II if requested					
DMB decision to proceed to Beta II		Program Manager			
		DMB			
Preparation for Milestone III					
Beta II Testing:					
Report due to DMB within two weeks of test completion		DMB			
JITC submits Joint Interoperability Certification Memo to DMB with final report and recommendation		Beta II Site			
ADM requesting Certificate to Field to DMB:		JITC and Beta II Site			
Request includes all items in previous ADM		Program Manager and MDA			
Test Reports from Beta II Testing		Program Manager			
Allow 2-4 weeks for DMB review process		Program Manager			
Provide Decision Briefing for Certificate to Field to DMB/DRB if requested		DMB			
DMB issues Certificate to Field		MDA or Designee			

MDA Milestone III Decision (Deployment Approval)		DMB			
--	--	-----	--	--	--

Figure C-4 Program Manager's Checklist

APPENDIX D

DMB MOBILE CODE POLICY

In February 1996, the DoDIIS ERB was tasked by the DMB to review the security aspects of the Sun Microsystems Java language and run-time application environment. Until a policy was established, no Java applets or applications were to be deployed.

In October 1996, the ERB drafted a policy on the use of Java (see ERB Home Page on Intelink). The policy was applicable to all applets/applications that transitioned across, or had the potential to transition across, network bounds. Specifically:

1. Commands, Sites and Program Management Offices were required to design, develop and implement only digitally signed Applets or applications.
2. Since digital signature technology was not currently commercially available, Commands, Sites and Program Management Offices were only to implement or deploy JAVA Applets or Applications that had been properly registered with the Intelink Service Management Center (ISMC) and that are hosted upon servers that are registered with the ISMC.
3. Community systems that were developed and deployed using Java technology were required to be tested for integrity assurance, identity and system administration training, prior to receiving the DMB mandated certification to field from the Joint Integration Test Facility.
4. Commands and Sites that provided non-migration systems using Java were responsible for ensuring their integrity and identity. Each Command or Site that developed Java applets or applications was to ensure that a process to test and assure quality of code was in place prior to deployment of the applet or application.

Also in October 1996, the Intelligence Systems Board (ISB), through the Senior Information Management (SIM) Panel, released its policy for the use of Java over Intelink. The policy applied specifically to the Intelink environment and did not constrain organizations from using applets in their enclaves. Furthermore, the policy was consistent with that being developed by the DMB. Specifically:

1. All Java applets used on Intelink are to be registered with the Intelink Service Management Center (ISMC).
2. Java applets can only be hosted on servers that are registered with the ISMC.
3. Organizations are expected to implement a code review and quality control process for deployed applets and are responsible for the Java applets that they deploy.
4. Organizations can run only "signed" Java applets on Intelink. Until such time as applet - signing" becomes commercially available, the following applied:

- a) Intelink-based processes, services, or information that were only available via Java applets were not to be deployed since they might become mission-critical. However, new Java applet capabilities that were not replacements for existing capabilities were not considered mission-critical since they were not previously available.
- b) Because there was still risk, consumer organizations were not to run Java applets on mission-critical systems.
- c) To minimize risks, organizations were advised to implement some means, such as a firewall, to filter out access to Java applets from external servers.
- d) Stand-alone Java programs were to be treated as any other software program would be treated.

In November 1996, the DMB issued its current policy on Java based on the recommendations of the ERB. The ERB recommendations were based on discussions with the Intelligence Systems Board and their work on the above policy. The DMB policy is applicable to all Java applets/applications that transition across, or have a potential to transition across, network bounds and executed without user intervention. The policy does not require the use of Java technology and it recognizes the right of each Command, Site or PM Office (PMO) to choose to implement or restrict this technology. Nothing in the policy relieves the Commands, Sites or PMs from conforming to existing DoD policies, standards, specifications, regulations, instructions and directives or any applicable laws. Specifically:

1. Commands, sites, and PMs are required to develop and implement digitally signed Java applets once this technology is commercially available, evaluated by the ERB, and approved by the DMB.
2. Since digital signature technology was not currently commercially available, Commands, Sites, and PMs are to only implement Java applets that have been properly registered with the ISMC. (NOTE: digital signature technology is now currently available but the public key infrastructure required to implement over Intelink is not.) Applets that do not transition the boundaries of the site local area network are exempted from this requirement.
3. Migration systems that are developed and implemented using Java technology are required to be tested for integrity assurance, identity, and system administration training, prior to receiving the DMB mandated certification to field from the Joint Integration Test Facility.
4. Non-migration system use of the Java language and run-time application environment will be the responsibility of the Command or Site to ensure integrity and identity. Each Command or Site that develops Java applets must ensure that a process to test and assure quality of code is in place prior to implementation of the applet.

DoD policy regarding mobile code can be found in DCID 6/3.

APPENDIX E

DII COE SPONSORSHIP

The Information contained in this Appendix was derived from information maintained by DISA.

- 1) **What is the definition of sponsorship?** Sponsorship is the process that a DoD community member uses to recommend a software product for inclusion into the DII COE. By sponsoring a product a community member is stating they will allocate appropriate level of resources to develop, operate, and maintain the product for the foreseeable future. Maintenance includes the implementation of enhancements, fixes, etc. requested by other community members.
- 2) **Who can sponsor a product?** Any of the voting members of the Architectural Oversight Group (AOG), to include Air Force, Army, Navy, Marines, Coast Guard, DISA, DoDIIS, and NIMA, can sponsor a product. Commands are represented by their lead service with exception of the J2s who work through DoDIIS. Sites, Program Managers, DEXAs, etc. cannot sponsor products.
- 3) **Which products can be sponsored?** Any Commercial Off the Shelf (COTS) product that satisfies *DII COE Integration & Run Time Specification* (I&RTS) integration requirements. GOTS products may be sponsored into the COE only if there is no acceptable 80% COTS solution and the product functionality does not duplicate existing COE functionality.
- 4) **Why sponsor a product?** DII COE philosophy is based on the concept of reuse and streamlined computer processes to eliminate redundant functionality and save DoD resources. Each community member sponsors segments of the DII COE for all of DoD to make use of, thus spreading development costs across DoD. Community members can then develop systems at a greatly reduced cost. A sponsored product also benefits from DISA providing additional levels of compliance and integration testing. DISA sometimes picks up funding for products used DoD wide.
- 5) **What does a community member have to do to sponsor a product?** Once the community member has identified a product to nominate to the DoD community they must answer yes to the following questions to proceed:
 - a) Does the product provide functionality useful to a majority of DoD?
 - b) If GOTS, no acceptable COTS solution?
 - c) If GOTS, no existing functionality already in the COE?
 - d) If GOTS, is it owned by the government, and is the source releasable?
 - e) Does the community have the resources to fund the product?
 - f) Is it Joint Technical Architecture (JTA) compliant?
 - g) Is it Y2K compliant?
 - h) Is or will the product be segmented to the appropriate level of compliance?
 - i) Does the community configuration management board (CMB) approve sponsorship?

6) **What is the process for sponsorship?** Once a community member has approved sponsorship of a product the following steps should occur:

- a) The Community Representative to the appropriate DII COE Technical Working Group (TWG) group initiates sponsorship process in the TWG.
- b) The Community Member Architecture Oversight Group (AOG) Representative briefs the AOG on product sponsorship.
- c) The TWG evaluates the product for the following:
 - Does this product provide functionality useful to a majority of DoD?
 - Does the product satisfy requirements specified in the Software Requirements Specification (SRS)?
 - Is it the best product available?
 - If GOTS, no acceptable COTS solution?
 - If GOTS, no existing functionality already in the COE?
 - Is it JTA compliant?
 - Is it Y2K compliant?
 - Is the product segmented to the appropriate level of compliance?
- d) If the product is selected by the TWG, the Chair schedules a design review with the DII COE Chief Engineer's Office.
- e) The Sponsoring Community is responsible for product documentation, design review package, change proposal, appropriate waivers (If any), and design review briefing.
- f) The product is briefed at a design review and, if acceptable, is added to the DRAFT DII COE Build Plan.
- g) The Build Plan is presented to AOG Executive Session (AOG ES) for recommendation to Configuration Review Control Board (CRCB) for approval.
- h) The CRCB approves the build plan and by inclusion of the product in the build plan, also approves the product.
- i) The Sponsoring Community delivers the product to DISA
- j) The Community Member performs ongoing maintenance and segmentation as necessary.
- k) The Community Member updates the product on a six-month cycle, as necessary

APPENDIX F

PUBLIC KEY INFRASTRUCTURE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

MEMORANDUM FOR SECRETARIES FO THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Interim Guidance for the Department of Defense (DoD) Public Key Infrastructure (PKI)

As the U. S. military and intelligence community redefine the way in which information will be accessed and used in the 21st century, the collective needs of the Warfighter, theatre commanders, support elements, and leaders at Defense and national levels must be addressed in the context of *Information Superiority*. The DoD PKI will provide the critical underpinning of our Information Assurance capabilities across the Department and thus our ability to achieve Information Superiority. Our ability to make consistent *risk management* decisions, in full consideration of the highly interconnected, interdependent, shared risk environment in which we conduct our daily operations, is inextricably linked to the services provided by the DoD PKI. Accordingly, I believe we must take an aggressive approach in establishing a PKI that meets our requirements for all information assurance services. The goal of this DoD-wide infrastructure is to provide general purpose PKI services, e.g., issue certificates supporting digital signature and encryption, provide directory services, enable the revocation of certificates, etc., to a broad range of applications, at the levels of assurance consistent with operational mission imperatives.

The DoD PKI must avoid the significant duplication of effort and costs that are incurred by unique and non-interoperable systems, enable the outsourcing of appropriate PKI activities and functions to achieve economics of scale, and must satisfy major program and operational requirements. Further, the DoD PKI must support the recovery of encryption keys for information as it traverses the network and while at rest. Finally, the PKI must comply with and support applicable DoD policies.

Within the next thirty- (30) days, the Information Assurance Directorate will staff three critical documents:

- a. DoD X.59 Certificate Policy
- b. DoD Certification Practice Statement
- c. DoD Public Key Infrastructure (PKI) Roadmap

These documents will contribute to establishing the enterprise-wide end-state for the DoD PKI, provide the foundation for our PKI strategy, and ensure that, Department-wide, we are consistent in identifying PKI assurance levels commensurate with mission objectives. They will establish the timeline for availability of PKI capabilities and ensure that we are able to outsource, as appropriate, functions supporting low value and non-mission critical transactions at the earliest possible time. It is essential that you give these documents the widest possible dissemination. Your comments will ensure that the DoD PKI strategy derived from this baseline meets, to the maximum extent possible, your operational mission requirements.

Until we have fully coordinated these documents and developed a Department-wide PKI strategy, no new certificate infrastructures shall be established without prior written approval of the DoD Chief Information Officer (CIO). Ongoing pilots may be continued but costs should be minimized and risk management decisions shall be thoroughly review by the designated Approving Authority (DAA) of the pilot to ensure that inappropriate risk to the interconnected networks has not been accepted.

Additional applications, beyond ongoing pilots, wishing to use the current medium assurance pilot infrastructure must, prior to implementation, conduct a risk assessment describing the services required from the infrastructure as well as the sensitivity of the information being protected. DISA and NSA will provide guidance concerning the information to be included in the risk assessment, and DoD PKI Senior Steering Committee will grant approval for use of the medium assurance infrastructure. In addition, these pilots will be required to report on their "lessons learned" from the pilot activities in support of enterprise-wide PKI decisions and plans. Guidance for the data to be reported by the pilot will be provided in the Roadmap document, mentioned above.

Our goal for establishing the *DoD PKI Strategy* and formal release of the referenced documents is January 15, 1999. My point of contact for this action is Richard C. Schaeffer, Jr., OASD (C3I), Director, Information Assurance, telephone: (703-695-8705).

//signed 12 August 1998 //
Arthur L. Money
Senior Civilian Official

Establishing the DoD PKI Strategy

Establishing the DoD & IC PKI Strategy

A public key infrastructure (PKI) comprises the people, policies, procedures, and computing / telecommunications resources needed to manage public key cryptography in computer networks. A PKI provides computer networks and their users with the following services: authentication, data integrity, non-repudiation, confidentiality, and (optionally) authorization.

A PKI supports "X.509 public key certificates," as defined in International Telecommunications Union - Telecommunications (ITU-T) Recommendation X.509. A public key certificate is a data structure that binds a subject (people, applications programs, machines, etc) and the subject's public key.

A private key is used to digitally sign data, such as messages, files, and transactions. The corresponding public key is used to verify the signature. A private key can also be used to decrypt data encrypted with the corresponding public key. In the DoD medium assurance PKI, the public/private key pairs used for non-repudiation or digital signature services are distinct from the pairs used for encryption/decryption services. Public/private key pairs are also used in algorithms that automatically distribute symmetric, secret keys.

X.509 public key certificates are signed and issued by a special user called a certification authority (CA). A CA may also revoke certificates. X.509 attribute certificates are signed, issued, and revoked by an attribute certificate issuer.

The DoD medium assurance PKI is authorized to protect unclassified and certain types of sensitive but unclassified (SBU) information, in accordance with the DoD Class 3 level of information assurance. The DoD medium assurance PKI may also be used for digital signature services, user authentication, and community of interest separation within certain types of classified networks, that is those which are protected by Type I cryptography. The U.S. DoD X.509 Certificate Policy specifies the permitted uses of a medium assurance (Class 3) PKI in encrypted and unencrypted networks.

The Intelligence Community is developing an IC PKI strategy under the IC Chief Information Officer (IC CIO). The IC PKI policy is still being developed and further guidance will be published soon.

More information regarding the DoD PKI strategy can be found in Draft "Internet X.509 Public Key Infrastructure PKIX Roadmap, <draft-ietf-pkix-roadmap-02.txt>, 23 June 1999. Information pertaining to Intelligence Community PKI activities can be found on Intelink at <http://www.iccio.ic.gov/>.

APPENDIX G

REFERENCES

G. 1 DoDIIS DOCUMENTS

G.1.1 General

- a) ASD/C3I, 10 February 1997, DOD Guide for Managing Information Technology as an Investment and Measuring Performance, Version 1.0.
- b) ASD/C3I, 14 May 1999, Memorandum, Implementation and Evolution of the Defense Information Infrastructure (DII) Common Operating Environment (COE).
- c) Chairman of the Joint Chiefs of Staff, July 1996, Joint Vision 2010, America's Military Preparing for Tomorrow.
- d) Chairman of the Joint Chiefs of Staff, 1997, National Military Strategy: Shape, Respond, Prepare Now—A Military Strategy for a New Era.
- e) Chairman of the Joint Chiefs of Staff, 10 August 1999, Instruction 3170.01A, Requirements Generation System.
- f) CMS, March 1999, DCI Strategic Intent for the United States Intelligence Community.
- g) Congress, 1993, Government Performance and Results Act of 1993.
- h) Congress, 1996, Clinger-Cohen Act/National Defense Authorization Act, Division E: Information Technology Management Reform, also known as the Information Technology Management Reform Act of 1996.
- i) DCI, March 1999, Strategic Intent for the United States Intelligence Community.
- j) DMB, April 1999, DoDIIS Enterprise Transition Methodology (DETM).
- k) DMB, September 1999, DRB Charter.
- l) DoDIIS SIMO White Paper, November 1996, Defining a Functional Reference Model for Intelligence (vol. 1 & 2).
- m) GAO Executive Guide, September 1997, Measuring Performance and Demonstrating Results of Information Technology Investments.

- n) Intelligence Systems Secretariat, November 1997, Intelligence Community Information Systems Strategic Plan, Enabling a More Agile Intelligence Enterprise FY1999-2003.
- o) International Organization of Standardization (ISO), 1995, ISO 12207, Software Life-Cycle Processes.
- p) International Organization of Standardization (ISO), 1998, ISO/IEC TR15271; Information Technology—Guide for ISO/IEC 12207.
- q) Institute of Electrical and Electronic Engineers (IEEE), 1995, EIA/IEEE J-STD-016-1995, Trial Use Standard—Electronic Industries Association, Software Development--Acquirer-Supplier Agreement.
- r) J2/Joint Staff, 1998, Battlespace Awareness J2 Campaign Plan: Implementing Joint Vision 2010.
- s) OSD, January 1993, DoD Manual 8320.1-M-1, Data Element Standardization Procedures.
- t) OSD, March 1994, DoD Manual 8320.1-M, DoD Data Administration Procedures.
- u) OSD, 1997, Requirements for Compliance with Reform Legislation for Information Technology Acquisitions Memorandum.
- v) OSD, 2 June 1997, Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106), Memorandum.
- w) The White House, 17 July 1996, Executive Order 13011, Federal Information Technology.
- x) The White House, October 1998, National Security Strategy for a New Century.

G.1.2 Acquisition

- a) ASD/C3I, 25 July 1997, Information Technology Investment Management Insight Policy for Acquisition.
- b) OSD, 25 October 1991, DoD Directive 5000.52, Education, Training, and Career Development Program.
- c) OSD, 18 November 1992, DOD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems.
- d) OSD, 15 March 1996, DoD Directive 5000.1, Defense Acquisition.

- e) OSD, 15 March 1996, DoD Directive 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System Acquisition Programs.
- f) OSD, 27 May 1997, DoD Directive 5000.35, Defense Acquisition Regulations Management.
- g) OSD, 30 December 1997, DoD Instruction 5200.40, Department of Defense Information Technology Certification and Accreditation Process (DITSCAP).
- f) Office of the Secretary of Defense, 1 May 1997, Requirements for Compliance with Reform Legislation for Information Technology (IT) Acquisitions (Including National Security Systems), Memorandum.

G.1.3 Technical Guidance

(Defense Information Infrastructure (DII) Common Operating Environment (COE) documentation can also be found at <http://spider.osfi.disa.mil/dii>)

- a) ASD/C3I, 23 June 1995, Defense Electronic Data Interchange Infrastructure Implementation, Memorandum.
- b) ASD/C3I, 29 April 1997, Use of the Ada Programming Language.
- c) ASD/C3I, 23 May 1997, Implementation of the Defense Information Infrastructure Common Operating Environment Compliance, Memorandum.
- d) Chairman of the Joint Chiefs of Staff, 30 June 1995, CJCS 6212.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems.
- e) DISA, 30 June 1994, DoD Human Computer Interface Style Guide, Volume 8 of the DoD Technical Architecture Framework for Information Management.
- f) DISA, 30 April 1996, DoD Technical Architecture Framework for Information Management, Volume 2: Technical Reference Model.
- g) DISA, 30 September 1996, DII COE Distributed Computing Environment Implementation Plan.
- h) DISA, 22 January 1997, DII COE Software Quality Compliance Plan.
- i) DISA, 1 April 1997, Configuration Management Plan.

- j) DISA, 8 March 1998, User Interface Specification for the Defense Information Infrastructure (DII).
- k) DISA, 26 May 1998, DoD Joint Technical Architecture, Version 2.0.
- l) DISA, 3 September 1999, DoD Joint Technical Architecture, Version 3.0, Draft.
- m) DISA, 1 April 1999, Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and RunTime Specification (I&RTS), v4.0, Draft.
- n) DMB, 17 September 1998, DoDIIS Profile of the DoD Joint Technical Architecture and Defense Information Infrastructure Common Operating Environment, Version 2.0.
- o) DoD, MIL-STD-973, April 1992, Configuration Management.
- p) MITRE, December 1997, Secure Windows NT Installation and Configuration Guide, Version 3.3, MTR 97W0000124.
- q) MITRE, December 1997, UNIX Configuration Guidance for the Defense Information Infrastructure (DII) Common Operating Environment (COE), Version 3.3, MP 97W000222.
- r) National Defense Authorization Act FY1996, Division E: Information Technology Management Reform, also known as the Information Technology Management Reform Act of 1996.
- s) Government Performance and Results Act of 1993.
- t) USD(A&T) and ASD/C3I, 22 August 1996, Implementation of the DoD Joint Technical Architecture, Memorandum.

G.1.4 Testing

- a) Air Force Rome Laboratory, Joint Integration Test Facility, 9 March 1999, Virtual Test Folder.
- b) Air Force 497th IG, 1 April 1999, Test and Evaluation Policy for DoDIIS Mission Application.
- c) Air Force 497th IG, 21 April 1999, Joint Integration Test Facility, DoDIIS Integration Requirements and Evaluation Procedures v2.0.
- d) Air Force Rome Laboratory Joint Integration Test Facility, 29 January 1998, Concept of Operations, Distributed Test Network.
- e) OSD, 23 February 1998, DoD Directive 5010.41, Joint Test and Evaluation Program.

G.1.5 Distribution

- a) JDISS JPO, 1999, Concept of Operations, DoDIIS Distribution Facility, Draft.
- b) JDISS JPO, 1999, Users Guide, DoDIIS Distribution Facility, Draft.
- c) JDISS JPO, 1999, Systems Administrators Guide, DoDIIS Distribution Facility, Draft.

G.1.6 Training

- a) DIA Regulation 24-11, 10 April 1995, Training: General Intelligence Training System.
- b) DoD MIL-HDBK-29612, 30 July 1999, Part 1, Guidance for Acquisition of Training Data Products and Services.
- c) DoD MIL-HDBK-29612, 30 July 1999, Part 2, Instructional Systems Development/Systems Approach to Training and Education.
- d) DoD MIL-HDBK-29612, 30 July 1999, Part 3, Development of Interactive Multimedia Instruction.
- e) DoD MIL-HDBK-29612, 30 July 1999, Part 4, Glossary for Training.
- f) OSD, 20 July 1984, DoD Directive 3305.2, DoD General Intelligence Training.
- g) OSD, 30 November 1988, DoD Directive 5000.53, Manpower, Personnel, Training, and Safety in the Defense System Acquisition Process.
- h) OSD, 14 March 1991, DoD Instruction 1322.20, Development and Management of Interactive Courseware for Military Training.
- i) MIL-PRF-29612A, 30 July 1999, Performance Specifications, Training Data Products.

G.1.7 Security

- a) DCI, 5 June 1999, DCID 6/3, Protecting SCI Within Information Systems.
- b) DIA, November 1993, DoDIIS Developer's Guide for Automated Information Systems (AIS) Security in DoD Intelligence Information Systems, SC-2610-142-93.
- c) DIA, November 1993, DoDIIS Site Information Systems Security Officer's Handbook, SC-2610-141-93.

- d) DIA, November 1993, DoDIIS Site Certifier's Guide, SC-2610-143-93.
- e) DIA, June 1995, DoDIIS Security Architecture Guidance and Directions (SAGD), Draft.
- f) DIA Manual 50-4, 30 April 1997, DoDIIS Information Systems Security (INFOSEC) Program.
- g) DIA & NSA, 17 March 1998, Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, FOUO.
- h) OSD, 21 March 1988, DoD Directive 5200.28, Security Requirements for Automated Data Processing Systems.

G.1.8 Budget

- a) DIA, 31 October 1998, General Defense Intelligence Program (GDIP) Program Manager's Guidance Memorandum (PMGM), Draft.
- b) DIA, 27 January 1999, Defense Intelligence Functional Manager Infrastructure, FY2001-2005 GDIP Infrastructure Technical and Cost Guidance.
- c) CMS and DASD (I&S), 1998, Joint Intelligence Guidance.
- d) OMB, 25 October 1996, Funding Information System Investments, Memorandum.

G.1.9 Messaging

- a) ASD/C3I, 18 October 1996, Policy Guidance for Defense Message System Implementation, Operation and Life-Cycle Management.
- b) Chairman of the Joint Chiefs of Staff, 31 July 1996, CJCS Instruction 6241.02, U.S. Message Text Formatting Policy and Procedures.
- c) Chairman of the Joint Chiefs of Staff, 01 May 1999, CJCSI 5721.01A, The Defense Messaging System and Associated Message Processing Systems.
- d) CMS, June 1999, Chief Information Officer, Intelligence Community Email Policy.
- e) CMS, 29 April 1998, Intelligence Community Defense Message System Management Office, Intelligence Community Defense Message System Requirements, v1.1.
- f) DISA, 1999, Defense Messaging System Design Architecture, Draft.

- g) DMB, 5 October 1999, DoDIIS AUTODIN Bypass System Operational Guidelines v1.0.
- h) DMB, 1999, DoDIIS AUTODIN Global Routing Plan, Draft.
- i) DMB, 1999, DoDIIS AUTODIN System Operating Instructions, Draft.
- j) DMB, 1999, DoDIIS AUTODIN System Implementation Plan, Draft.
- k) DMB, 1999, DoDIIS AUTODIN Security Implementation Plan, Draft.

APPENDIX H

GLOSSARY OF ACRONYMS

ADM	Acquisition Decision Memorandum
AIS	Automated Information System
AOG	Architectural Oversight Group
APB	Acquisition Program Baseline
API	Application Programming Interface
ASD	Assistant Secretary of Defense
AUTODIN	Automatic Digital Network
BES	Budget Estimate Submission
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
C4ISR	C4I Surveillance and Reconnaissance
CA	Certifying Authority
CAIV	Cost as an Independent Variable
CAS	Consolidated Applications Server
CCP	Consolidated Cryptologic Program
CI	Controlled Interface
CIAP	CIA Program
CIO	Chief Information Officer
CJCSI	Chairman Joint Chiefs of Staff Instruction
CM	Configuration Management
CMB	Configuration Management Board
COE	Common Operating Environment
CONOPS	Concept of Operations
COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CRCB	Configuration Review Control Board
CRD	Capstone Requirements Document
CSE	Client Server Environment
CSE-SS	CSE System Services
CSP	Communication Support Processor
DAA	Delegated Acquisition Authority
DCE	Distributed Computing Environment
DCI	Director Central Intelligence
DCID	Director Central Intelligence Directive
DCOM	Distributed Component Object Modules
DDF	DoDIIS Distribution Facility
DEC	Digital Equipment Corporation
DEPSECDEF	Deputy Secretary of Defense

DETM	DoDIIS Enterprise Transition Methodology
DExA	DoDIIS Executive Agent
DIA	Defense Intelligence Agency
DIAM	DIA Manual
DIFM	Defense Intelligence Functional Manager
DIFM-I	Defense Intelligence Functional Manager-Infrastructure
DII	Defense Information Infrastructure
DII COE	Defense Information Infrastructure Common Operating Environment
DITP	Defense Intelligence Tactical Program
DISA	Defense Information Systems Agency
DMB	DoDIIS Management Board
DMS	Defense Message System
DoD	Department of Defense
DoDD	DoD Directive
DoDIIS	DoD Intelligence Information Systems
DPL	DoDIIS Product List
DRB	DMB Review Board
DR/DIA	Director, DIA
DTG	Date/Time Group Enhancement and Modernization (JEM)
EDRB	Expanded Defense Resources Board
ERB	Engineering Review Board
FAT	Factory Acceptance Test
FRM-I	Functional Reference Model for Intelligence
FY	Fiscal Year
FYDP	Five Year Development Plan
GCCS	Global Command and Control System
GDIP	General Defense Intelligence Program
GITC	General Intelligence Training Council
GITS	General Intelligence Training System
GOTS	Government Off-the-Shelf
HP	Hewlett Packard
HTML	Hyper Text Markup Language
IAW	in accordance with
IC	Intelligence Community
ICD	Interface Control Document
ICDMO	Intelligence Community DMS Management Office
ICWG	Interface Control Working Group
IEEE	Institute of Electrical and Electronics Engineers
IG	Intelligence Group
IM	Information Management

IMA	Intelligence Mission Application
INFOSEC	Information Security
IPAT	In-Plant Acceptance Testing
IPDM	Intelligence Program Decision Memorandum
IPOM	Intelligence Program Objective Memorandum
I&RTS	Integration and Runtime Specifications
IRS	Interface Requirement Specification
ISB	Intelligence Systems Board
ISMC	Intelink Service Management Center
ISO	International Organization of Standardization
IT	Information Technology
ITMRA	Information Technology Management Reform Act
ITU-T	International Telecommunications Union - Telecommunications
JADE	JIVA Analytic Data Environment
JDCSISS	Joint DoDIIS/Cryptologic SCI Information Systems Security Standards
JDISS	Joint Deployable Intelligence Support Services
JDISS JPO	JDISS Joint Program Office
JIEO	Joint Interoperability and Engineering Organization
JIMO	JIVA Integration Management Office
JITC	Joint Interoperability Testing Command
JITF	Joint Integration Test Facility
JIVA	Joint Intelligence Virtual Architecture
JMIP	Joint Military Intelligence Program
JMITC	Joint Military Intelligence Training Center
JROC	Joint Requirements Oversight Council
JTA	Joint Technical Architecture
JTRR	Joint Test Readiness Review
JWICS	Joint Worldwide Intelligence Communications System
KPP	Key Performance Parameters
LAN	Local Area Network
MAIS	Major Automated Information System Managers
MBB	Mission Based Budgeting
MCEB	Military Communications-Electronics Board
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Programs
MIB	Military Intelligence Board
MNS	Mission Needs Statement
MOP	Memorandum of Policy
NFIP	National Foreign Intelligence Program
NIMA	National Imagery and Mapping Agency

NIMC	National Imagery and Mapping College
NIMAP	National Imagery and Mapping Agency Program
NIPRNET	Unclassified but Sensitive IP Router Network
NITFS	National Imagery Transmission Format Standard
NSA	National Security Agency
OI	Operating Instructions
O&M	Operations and Maintenance
ORD	Operational Requirements Document
OSs	Operating Systems
OSD	Office of the Secretary of Defense
PAO	Project Action Officer
PEO	Program Executive Officer
PKI	Public Key Infrastructure
PM	Project Manager
PMGM	Program Managers Guidance Memorandum
PMO	Project Management Office
PMP	Program (or Project) Management Plan
POI	Program of Instruction
SAP	Site Activation Plan
S&T	Scientific & Technical
SAGD	Security Architecture Guidance and Directions
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SHADE	Shared Data Environment
SIM	System Integration Management
SIMHWG	Special Intelligence Message Handling Working Group
SIMO	System Integration Management Office
SIO	Service Intelligence Office
SIPRNET	Secret IP Router Network
SRS	Software Requirements Specification
SRTM	Security Requirements Traceability Matrix
STP	Site Transition Plans
T&E	Test and Evaluation
TBD	To be determined
TIARA	Tactical Intelligence and Related Activities
TMP	Training Management Plan
TOSs	Target Operating Systems
TRR	Test Readiness Review
TWG	Technical Working Group
URL	Uniform Resource Locator
USMTF	United States Message Text Format

WNT	Windows New Technology
Y2K	Year 2000